Risk-Based Cost-Benefit Analysis: Method and Example Applications

Presented at the INCOSE Enchantment Chapter Member Meeting

November 9, 2011

By Gregory D. Wyss, Ph.D.
Distinguished Member of Technical Staff
Sandia National Laboratories

Research Team: **Gregory D. Wyss, John P. Hinton, Katherine Dunphy Guzman, John Clem, Consuelo Silva and Kim W. Mitchiner**

Contact: ☎ (505) 844-5893 💻 gdwyss@sandia.gov

Sandia National Laboratories is a multi-program laboratory managed and operated by Sandia Corporation, a wholly owned subsidiary of Lockheed Martin Corporation, for the U.S. Department of Energy's National Nuclear Security Administration under contract DE-AC04-94AL85000.

The materials in this presentation are taken from SAND2009-4307C, SAND2010-3549C, and SAND2011-4351C, which have been approved for Unlimited Release

3 Words and Their Meanings

Safety

Security

Risk

3 Words and Their Meanings

Safety

Security

Risk

“Potential for an unwanted outcome resulting from an incident, event, or occurrence,
as determined by its likelihood
and the associated consequences”

DHS Risk Lexicon, Sept. 2008, p. 24

A Typical Definition of Risk

Scenario	Consequence	Likelihood
S_1	C_1	F_1
S_2	C_2	F_2
S_3	C_3	F_3
S_4	C_4	F_4
S_5	C_5	F_5
S_6	C_6	F_6
…	…	…

This *table*
***IS* the risk!**

– **Risk can be thought of as answers to 3 questions:**

- ***What can happen?*** ***(scenario)***
- ***How likely is it?*** ***(probability / frequency)***
- ***How bad is it?*** ***(consequence)***

"If [a] table contains all the scenarios we can think of, we can then say that it (*the table*) is the answer to the question and therefore *is the risk*."

Kaplan & Garrick, Risk Analysis 1:1(11) 1981, emphasis added.

Risk for a Scenario:

$$R = \underbrace{P_A \cdot \left(1 - P_E\right)}_{\text{How likely?}} \cdot \underbrace{C}_{\text{How bad?}}$$

A Typical Definition of Risk

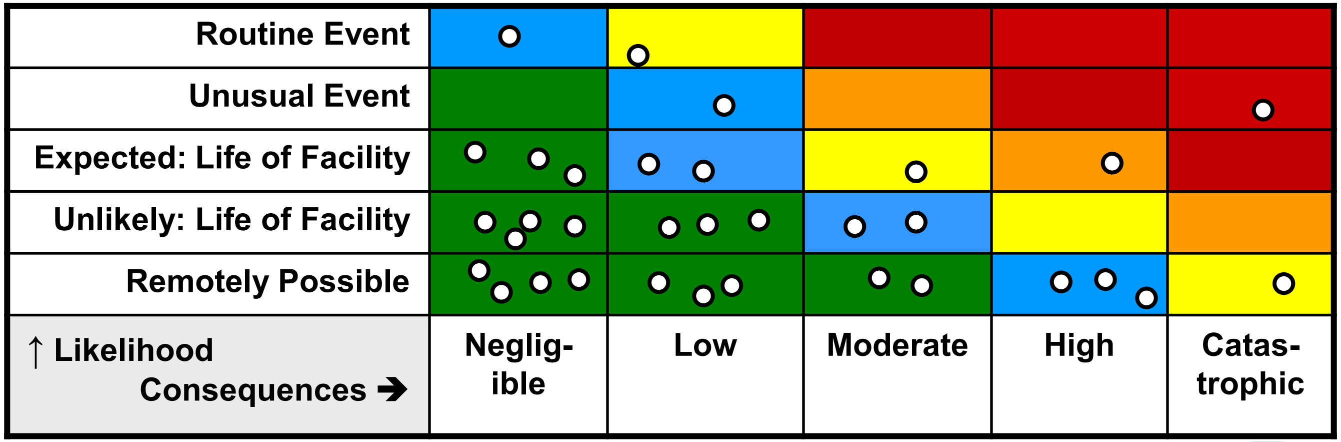
Scenario	Consequence	Likelihood
S_1	C_1	F_1
S_2	C_2	F_2
S_3	C_3	F_3
S_4	C_4	F_4
S_5	C_5	F_5
S_6	C_6	F_6
…	…	…

This *table* / *IS* the risk!

– Risk can be thought of as answers to 3 questions:
- ***What can happen?*** *(scenario)*
- ***How likely is it?*** *(probability / frequency)*
- ***How bad is it?*** *(consequence)*

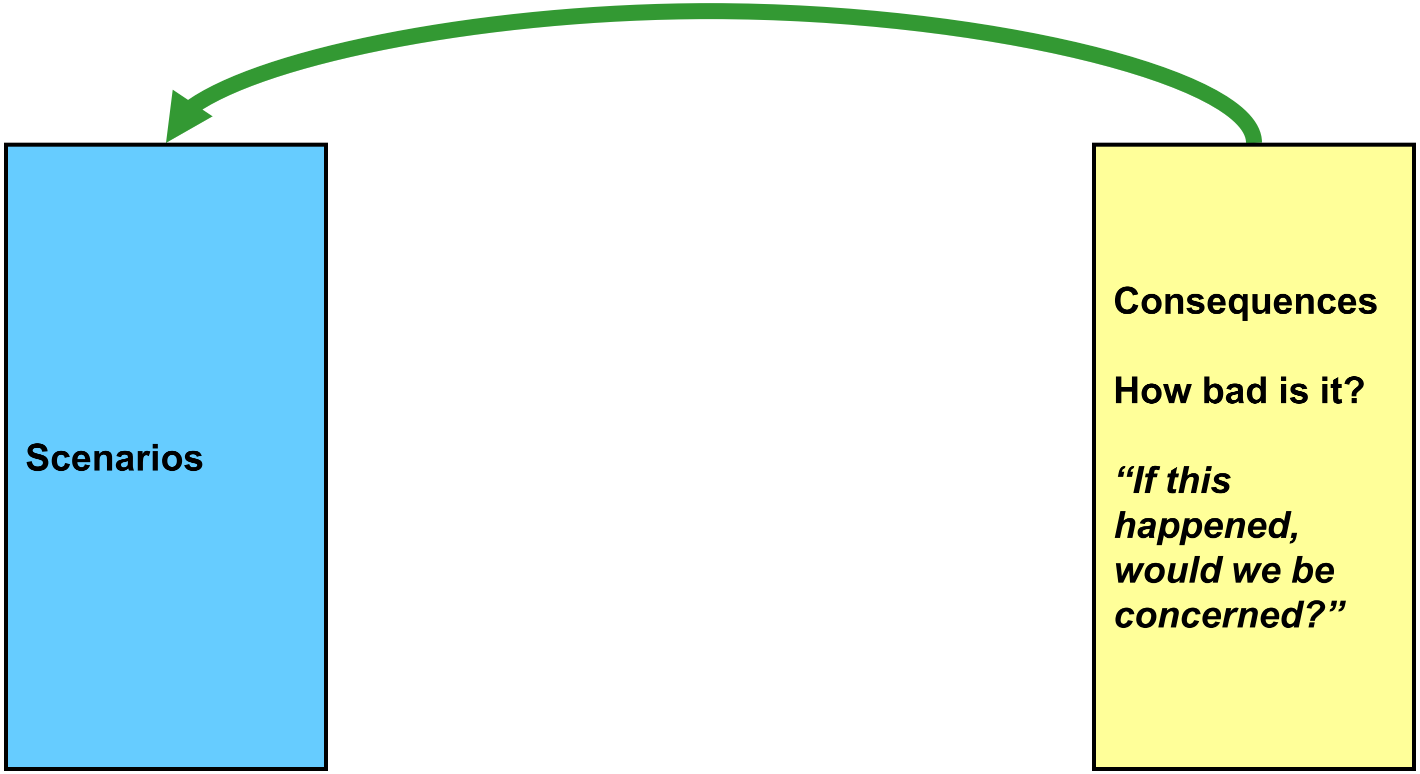
> **"If [a] table contains all the scenarios we can think of, we can then say that it (*the table*) is the answer to the question and therefore *is the risk*."**

Kaplan & Garrick, Risk Analysis 1:1(11) 1981, emphasis added.



Routine Event	🟦 ○	🟨 ○	🟥	🟥	🟥
Unusual Event	🟩	🟦 ○	🟧	🟥	🟥 ○
Expected: Life of Facility	🟩 ○ ○ ○	🟦 ○ ○	🟨 ○	🟧 ○	🟥
Unlikely: Life of Facility	🟩 ○ ○ ○ ○	🟩 ○ ○ ○	🟦 ○ ○	🟨	🟧
Remotely Possible	🟩 ○ ○ ○ ○	🟩 ○ ○ ○	🟩 ○ ○	🟦 ○ ○ ○	🟨 ○
↑ Likelihood Consequences →	**Neglig-ible**	**Low**	**Moderate**	**High**	**Catas-trophic**

Risk Assessment Overview



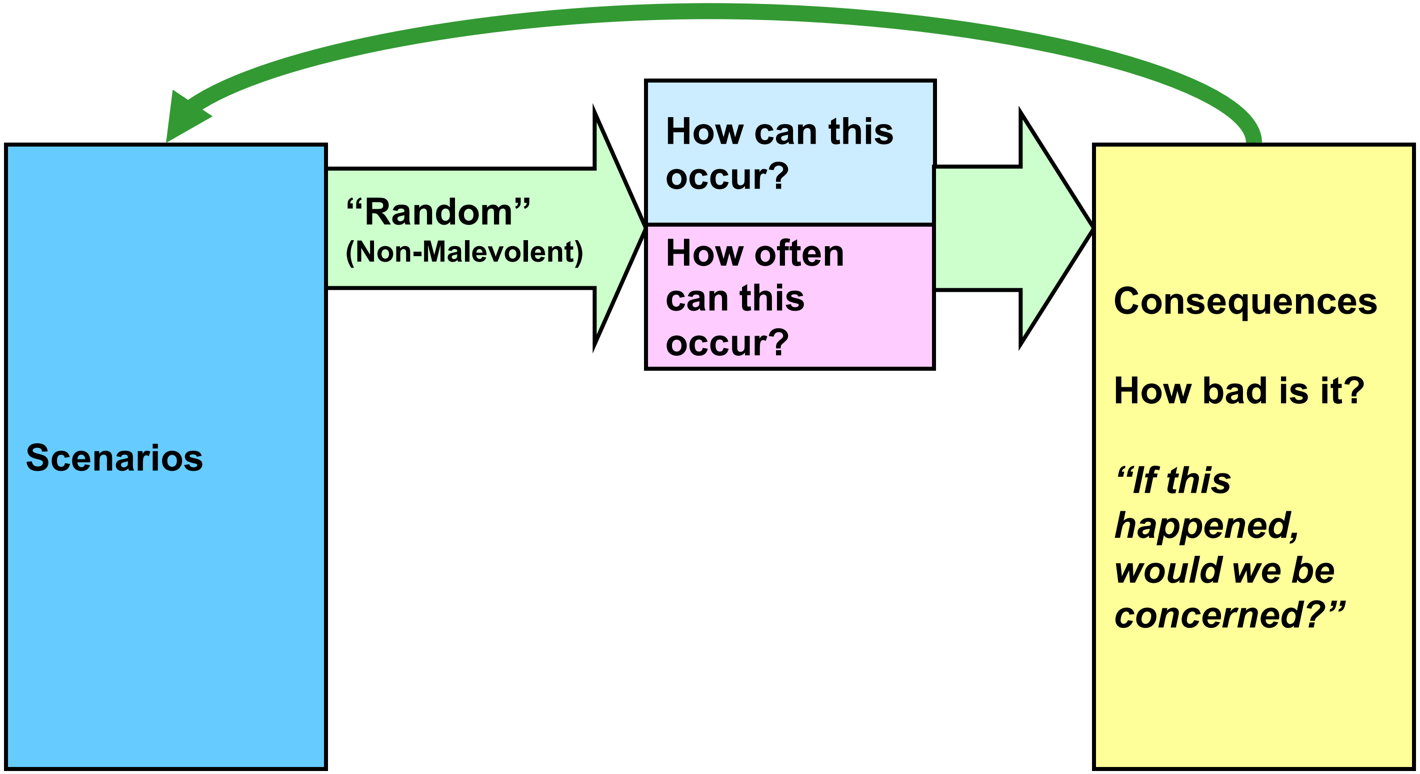
Scenarios

Consequences

How bad is it?

"If this happened, would we be concerned?"

Risk Assessment Overview



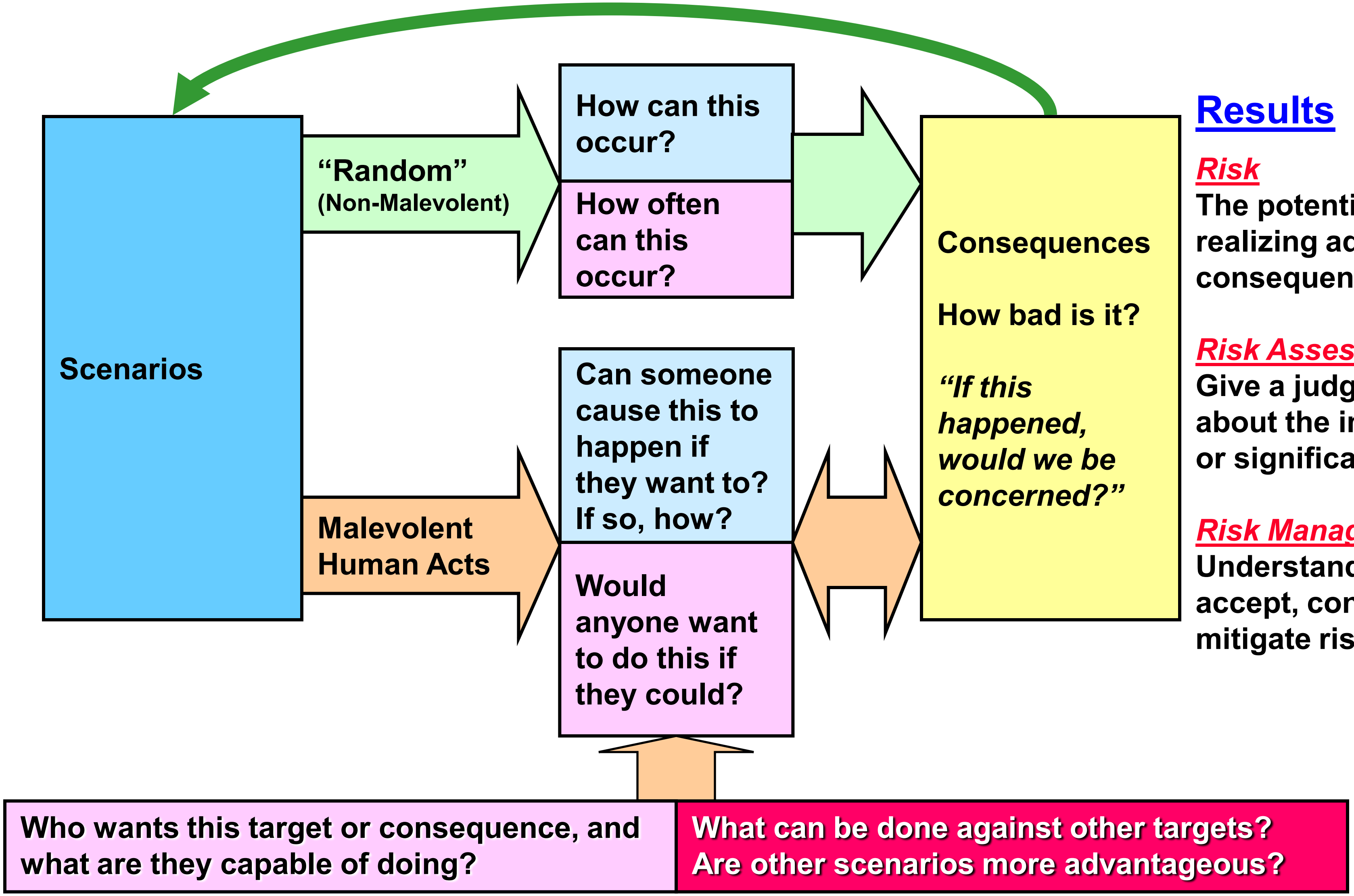
Results

Risk
The potential for realizing adverse consequences

Risk Assessment
Give a judgment about the importance or significance of risk

Risk Management
Understand and accept, control, or mitigate risk

Risk Assessment Overview



Scenarios

“Random”
(Non-Malevolent)

How can this occur?

How often can this occur?

Malevolent Human Acts

Can someone cause this to happen if they want to? If so, how?

Would anyone want to do this if they could?

Consequences

How bad is it?

“If this happened, would we be concerned?”

Who wants this target or consequence, and what are they capable of doing?

What can be done against other targets? Are other scenarios more advantageous?

Results

Risk
The potential for realizing adverse consequences

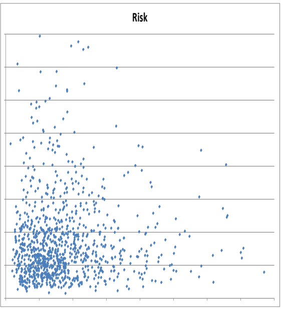
Risk Assessment
Give a judgment about the importance or significance of risk

Risk Management
Understand and accept, control, or mitigate risk

Security Risk vs. Safety Risk

Scenario	Consequence	Likelihood
S_1	C_1	F_1
S_2	C_2	F_2
S_3	C_3	F_3
S_4	C_4	F_4
S_5	C_5	F_5
S_6	C_6	F_6
…	…	…

This *table* *IS* the risk!



<table>
<tr><th></th><th colspan="2">Safety</th><th>Security</th></tr>
<tr><td>Consequences</td><td colspan="2"><i>f</i>(system, environment)</td><td><i>f</i>(√,√, adversary capability)</td></tr>
<tr><td>Likelihood of a Scenario</td><td colspan="2"><i>f</i>(system, environment)
~Independent of other scenarios that exist (at least outside the system)</td><td><i>f</i>(√,√, adv. capability & intent, consequence, similar systems)
Strongly dependent on other scenarios that exist – <i><u>both</u></i> inside and outside the system</td></tr>
<tr><td>Initiators</td><td colspan="2">Random</td><td>Deliberate
(e.g., cause a safety scenario)</td></tr>
<tr><td>Human Actions</td><td colspan="2">Benevolent</td><td>Benevolent, Malevolent</td></tr>
<tr><td>Likely Causes for Events</td><td>↑↑(↑)
↑↑(↑)
↑
↓</td><td>Human Actions
Active Components
Adverse Environments
Passive Components</td><td>↑↑↑
↑↑↑
↓ or ↑↑↑
↑↑↑</td></tr>
<tr><td>Observability of Precursors</td><td colspan="2">May be observable and/or predictable</td><td>Deliberately concealed</td></tr>
</table>

Security Risk Management Recommendations from the National Academy of Sciences

- **Our goal must be** ***effective security risk management.***

National Academy of Sciences, 2010, emphasis added

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

- **Key risk management recommendations include:**
  - Focus on risk management rather than "how much or little risk exists"
  - Qualitative risk assessment methods may be suitable
  - Use a risk-informed, not risk *based*, approach to security risk management
    - Informed by PRA *tools*, but not relying on PRA

Goal: Manage Security Risks

- Problem: attack likelihoods are highly uncertain and change rapidly.
  - Depends on attacker's capability, motivation & intent
  - Depends on attacker's other opportunities inside ***and*** outside the system.
  - Predicting likelihood makes risk hard to use for security decision making

- A different risk management approach: examine adversary criteria for selecting which attack scenario to pursue, including:

Adversary's Decision Criterion	How we make an attack less likely
"Could I do it if I wanted to?" *(Is success likelihood high?)*	
"Would I do it if I could?" *(Worthy investment of resources?)* *(Does it violate my doctrine?)*	
"Are the expected consequences high enough?"	

Goal: Manage Security Risks

- Problem: attack likelihoods are highly uncertain and change rapidly.
  - Depends on attacker's capability, motivation & intent
  - Depends on attacker's other opportunities inside *and* outside the system.
  - Predicting likelihood makes risk hard to use for security decision making

- A different risk management approach: examine adversary criteria for selecting which attack scenario to pursue, including:

Adversary's Decision Criterion	How we make an attack less likely
"Could I do it if I wanted to?" *(Is success likelihood high?)*	Make attack scenario more difficult
"Would I do it if I could?" *(Worthy investment of resources?)* *(Does it violate my doctrine?)*	Make attack scenario more difficult or reduce potential consequences
"Are the expected consequences high enough?"	Reduce the potential or expected consequences of the scenario

Attack scenarios:

Easy

&

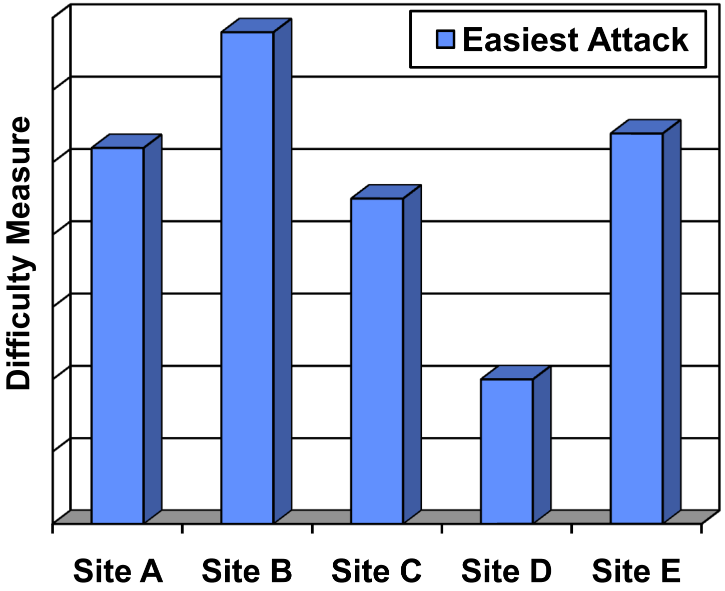
High-Consequence

=

High Risk

Security Risk Management: Making Easy Attacks More Difficult

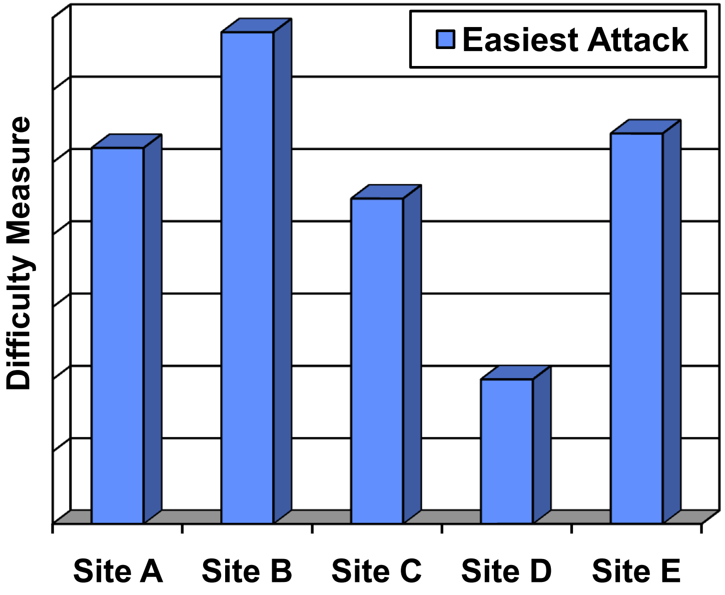
Illustration based on sites assumed to have the ***same consequence*** *for a successful attack.*



- **Are sites balanced?**
- **Where should I spend my next dollar?**

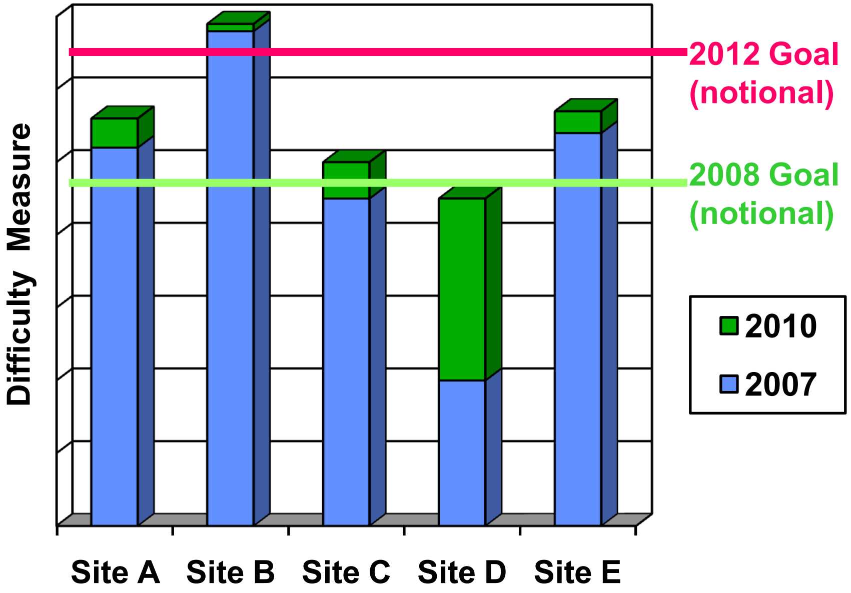
Security Risk Management: Making Easy Attacks More Difficult

*Illustration based on sites assumed to have the **same consequence** for a successful attack.*

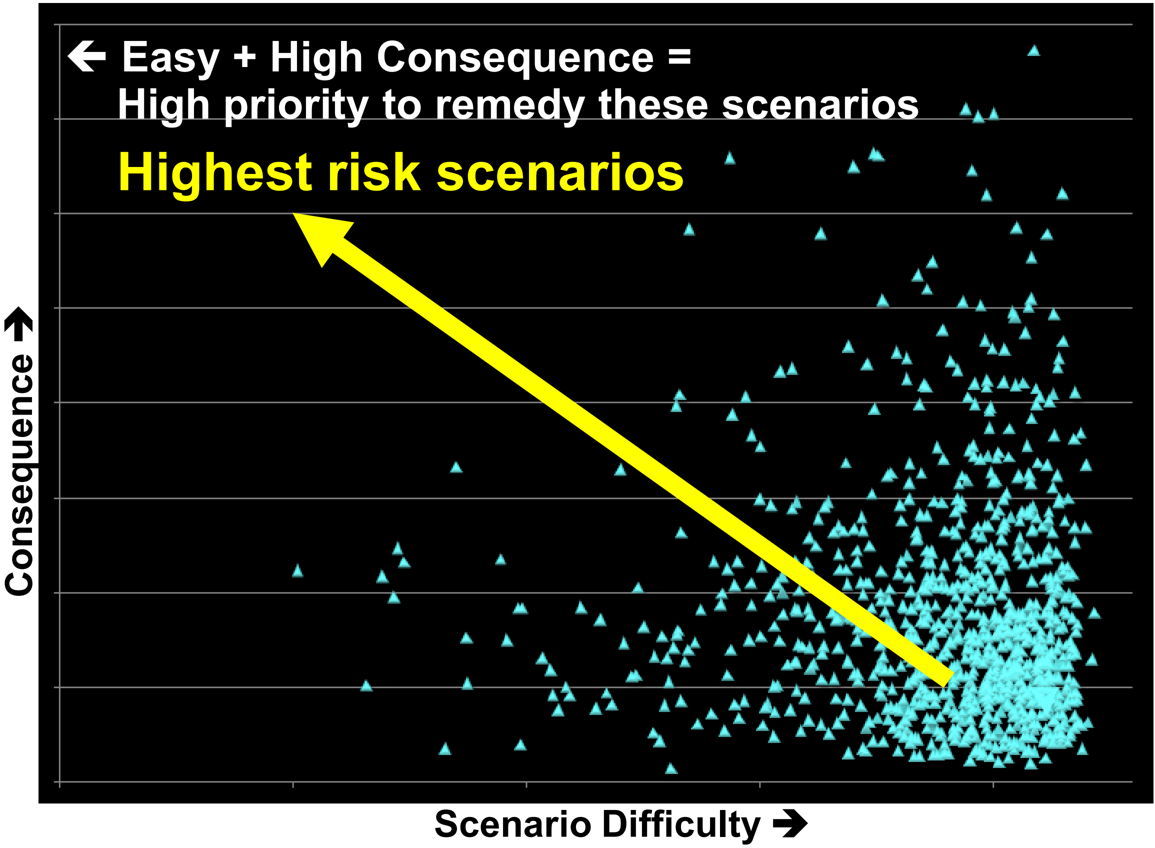


- Are sites balanced?
- Where should I spend my next dollar?

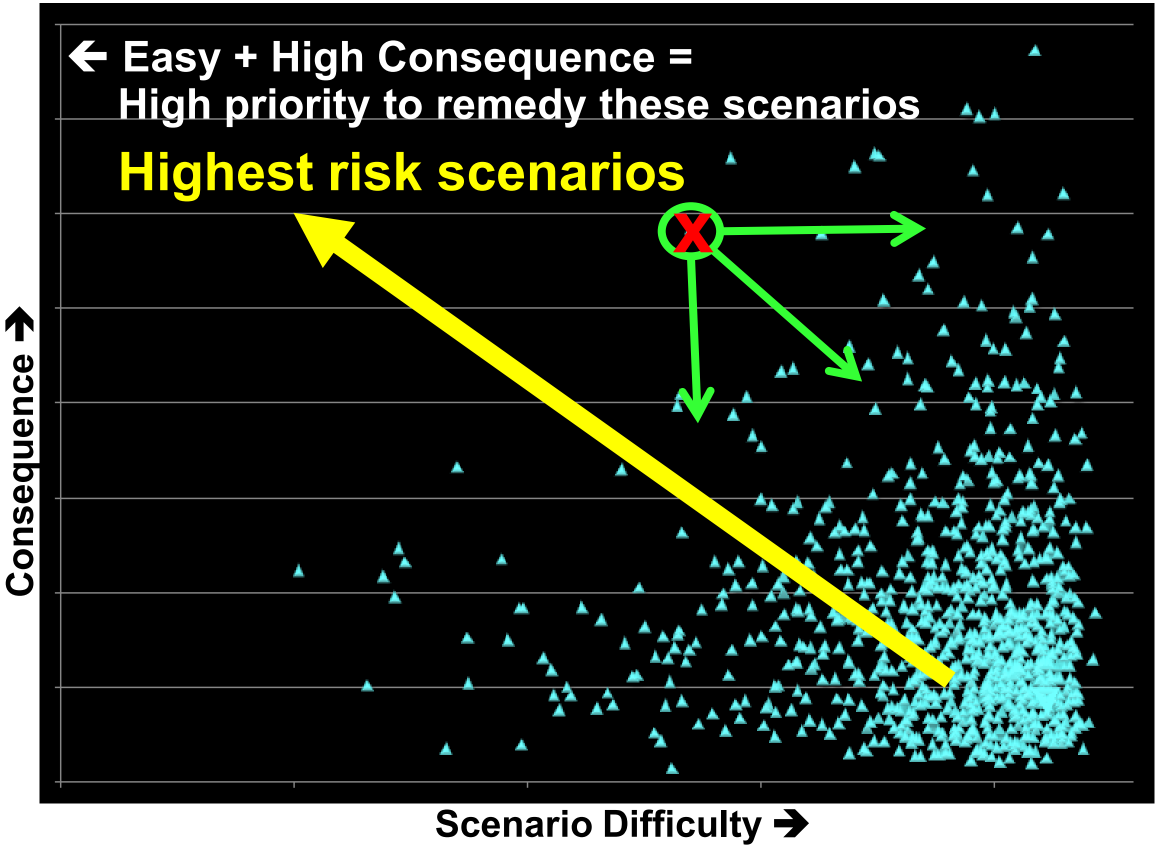
- How much have I improved?
- Why do my sites not meet the new security goal?



The Next Step: Manage Risk with Both Scenario Difficulty *and* Consequence



The Next Step: Manage Risk with Both Scenario Difficulty *and* Consequence



To "fix" a scenario we must

- Eliminate it (make it impossible to achieve)
- Reduce the consequences if it is completed
- Make it harder to accomplish successfully

… or any combination of these

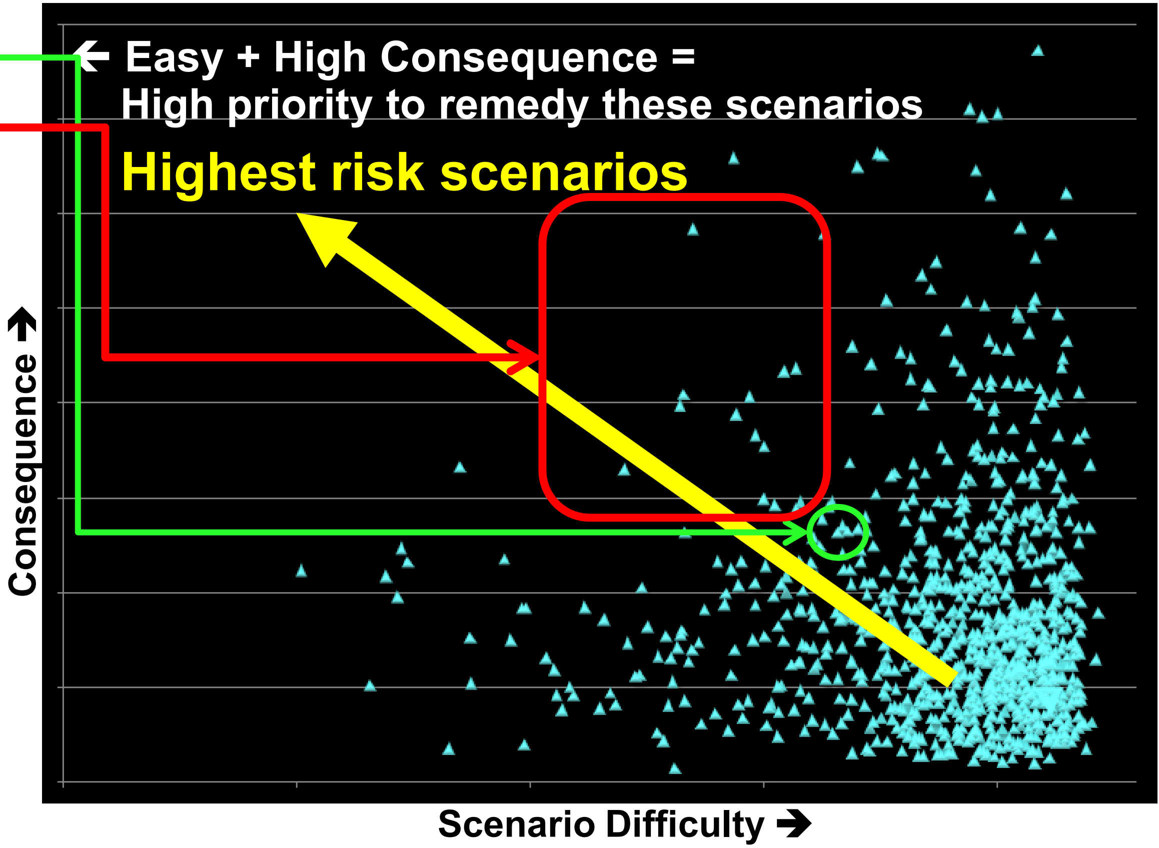
The Next Step: Manage Risk with Both Scenario Difficulty *and* Consequence

If we fix this…

Without fixing this…

We may not have improved security. *Because…*

Many scenarios still exist that are both easier to achieve AND provide higher consequences!



Why use scenario difficulty in security risk management?

- Difficulty better reflects the adversary planning process
- Difficulty changes more slowly and predictably than likelihood
- Problem: How do we assess the difficulty of an attack?

To "fix" a scenario we must

- Eliminate it (make it impossible to achieve)
- Reduce the consequences if it is completed
- Make it harder to accomplish successfully

… or any combination of these

Considerations for Estimating Attack Scenario Difficulty

Attack Preparation

- **Outsider attack participants**
  - *Number of engaged participants*
  - *Training & expertise required*
- **Insider attack participants**
  - *Number and coordination*
  - *Level of physical and cyber access required, sensitivity, vs. security controls*
- **Organizational support structure**
  - *Size, capabilities & commitment*
  - *Training facilities, R&D, safe haven, intelligence & OPSEC capabilities…*
- **Availability of required tools**
  - *Rarity, signatures for intelligence or law enforcement, training signatures…*

Attack Execution

- **Ingenuity & inventiveness**
- **Situational understanding**
  - *Observability & transience of vulnerabilities*
- **Stealth & covertness**
- **Dedication & commitment of participants**
  - *Risk to both outsiders & insiders includes personal risk, willingness to die, etc.*
  - *Risk to the "cause" or support base*
- **Operational complexity/flexibility**
  - *Precision coordination of disparate tasks*
  - *Multi-modal attack (cyber+physical+???)*

Example characteristics used to establish levels of difficulty for each dimension:*

Level 1		Level 3		Level 5
Easily accessible to general public by legal means w/o special skills		Requires capability similar to organized criminal, paramilitary or terrorist enterprise		Requires state-supported capability & specialized skills; typically accessible only by elite forces

*Additional details can be found in the paper.

Considerations for Estimating Attack Scenario Difficulty

Attack Preparation

- **Outsider attack participants**
  - *Number of engaged participants*
  - *Training & expertise required*
- **Insider attack participants**
  - *Number and coordination*
  - *Level of physical and cyber access required, sensitivity, vs. security controls*
- **Organizational support structure**
  - *Size, capabilities & commitment*
  - *Training facilities, R&D, safe haven, intelligence & OPSEC capabilities…*
- **Availability of required tools**
  - *Rarity, signatures for intelligence or law enforcement, training signatures…*

Attack Execution

- **Ingenuity & inventiveness**
- **Situational understanding**
  - *Observability & transience of vulnerabilities*
- **Stealth & covertness**
- **Dedication & commitment of participants**
  - *Risk to both outsiders & insiders includes personal risk, willingness to die, etc.*
  - *Risk to the "cause" or support base*
- **Operational complexity/flexibility**
  - *Precision coordination of disparate tasks*
  - *Multi-modal attack (cyber+physical+???)*

Scenario difficulty is a property of the *target.*
It estimates how capable the adversary must be to have a successful attack.

Risk managers can then ask, "Are the easiest attacks difficult enough to deter the adversaries we are concerned about?"

**Additional details can be found in the paper.*

Less Difficulty Example Scenario: Oklahoma City Bombing

This scenario reflects the difficulty that was likely encountered by the participants in the plot to bomb the Murrah Federal Building in Oklahoma City.

Level ***(Score)*** *[1, 2, 3, 4, 5 → 1, 3, 9, 27, 81]*

Attack Planning & Preparation	Participants	2 *(3)*	Several (~2-5); Small team
	Training	2 *(3)*	Self-taught; Open source info; No professional foundation; Practice not required for critical tasks
	Support	1 *(1)*	Minimal; Few if any support personnel / collaborators; No intelligence support; Preparations easily concealed—no need for cover; Open source info
	Tools	2 *(3)*	Legal availability controlled, limited to special purpose uses; Typical of criminal enterprises
	# of Insiders	1 *(1)*	None
	Insider Access	1 *(1)*	None
	Ingenuity	1 *(1)*	Very predictable, straightforward approach; Easily conceivable by knowledgeable public; Defenses likely to be well prepared / trained against
Attack Execution	Situational Understanding	1 *(1)*	Minimal; Requires little recognition or utilization of exploitable conditions; Exploitable vulnerabilities are persistent and predictable, with evident signatures
	Stealth & Covertness	1 *(1)*	Minimal
	Outsider Commitment	2 *(3)*	Persistent remote exposure or participants, limited direct exposure to less-than-lethal conditions; Little risk of casualties, but significant risk of participant attribution
	Insider Commitment	1 *(1)*	None
	Complexity	1 *(1)*	Single avenue of attack with simple tasks; Unimodal tasks; If multi-modal attack, modalities are sequential, temporally decoupled
	Flexibility	1 *(1)*	Singular binary course of action; No contingency planning; Little tactical adjustment
Aggregated Score		**-- *(21)***	*Score for each level is 3x that of the next lower level in this example.*

Moderate Difficulty Example: Cyber Theft of Personal Information

A group wishes to steal personal information from an enterprise with reasonable cyber defenses. Attackers learn which individuals are responsible for maintaining the cyber defenses, and send them "spear pfishing" emails that install special malware. Attackers use this initial access to escalate privileges and steal information.

Attack Planning & Preparation	Participants	2 *(3)*	Several (~2-5); Small team
	Training	3 *(9)*	Professionally trained in most critical task areas; Some deep expertise
	Support	1 *(1)*	Minimal; Few if any support personnel / collaborators; No intelligence support; Preparations easily concealed—no need for cover; Open source info
	Tools	1 *(1)*	Legally available to public on open market; Improvised from legal elements
	# of Insiders	1 *(1)*	None
	Insider Access	1 *(1)*	None
	Ingenuity	2 *(3)*	Rare but known approach; At least one instance of historical use of approach (but not many instances); Defenses may be prepared / trained against
Attack Execution	Situational Understanding	2 *(3)*	Exploitable vulnerabilities are persistent and predictable, but signatures require persistent and/or skillful observation to recognize; Opportunistic adaptation may decrease adversary risk for the scenario, but are probably not required for adversary success.
	Stealth & Covertness	3 *(9)*	Requires some subterfuge / ruse within defenders' observational purview
	Outsider Commitment	2 *(3)*	Persistent remote exposure or participants, limited direct exposure to less-than-lethal conditions; Little risk of casualties, but significant risk of participant attribution
	Insider Commitment	2 *(3)*	Minimal personal risk; Potentially unintentional; Can be independently acquired or corroborated; Temporally decoupled from attack
	Complexity	2 *(3)*	Single avenue of attack with a complex task; If multi-modal tasks, modalities are temporally decoupled are loosely coordinated
	Flexibility	2 *(3)*	***Between*** "Singular binary course of action; No contingency planning; Little tactical adjustment" ***and*** "Some adaptation required, during the planning process"
Aggregated Score		**-- *(43)***	*Score for each level is 3x that of the next lower level in this example.*

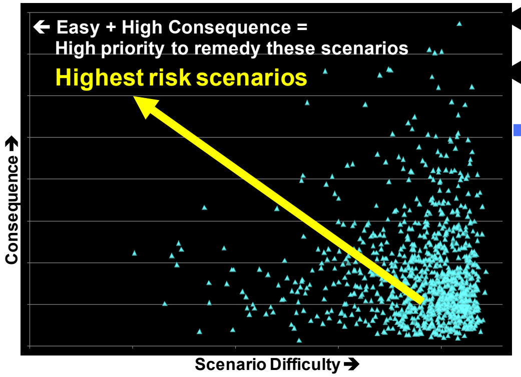
High Difficulty Example: Sabotage at a High Security Temporary Facility

A high-value item is stored in a temporary remote high security location. Adversaries pre-emplace themselves “under the noses” of the defenders and execute a precisely coordinated attack among multiple teams. The environment is unpredictable due to randomness that is inherent in the security plans. An insider provides information but does not assist directly in the attack.

Attack Planning & Preparation	Participants	3 *(9)*	Handful (~6-12); Large team or Few small teams
	Training	3 *(9)*	Professionally trained in most critical task areas; Some deep expertise
	Support	4 *(27)*	Large; One-few 100’s support personnel; Multiple compartmented support teams of professionals / specialists for training; Professional sub-state intelligence network; Sophisticated organization for cover
	Tools	3 *(9)*	Mixed bag; Typical of insurgency, paramilitary, terrorist enterprises
	# of Insiders	3 *(9)*	One
	Insider Access	3 *(9)*	Moderate; Requires intentional actions by insider with access to moderately protected security features; Contribution requires intentional compromise of at least one significant security control (e.g. portal monitoring, access authorizations, etc.)
	Ingenuity	3 *(9)*	Logical but not anticipated approach; No instances of historical use of approach; Only extensively trained defense would be prepared / trained against
Attack Execution	Situational Understanding	2 *(3)*	Exploitable vulnerabilities are persistent and predictable, but signatures require persistent and/or skillful observation to recognize; Opportunistic adaptation may decrease adversary risk for the scenario, but are probably not required for adversary success.
	Stealth & Covertness	4 *(27)*	Requires undetected operations over significant period of time within defenders’ observational purview
	Outsider Commitment	3 *(9)*	Persistent, direct exposure of participants; Requires selfless team sacrifice; Survival of participants not expected; Some fatalities certain; Direct attribution likely, supporter anonymity uncertain
	Insider Commitment	1 *(1)*	None
	Complexity	4 *(27)*	Multiple avenues requiring precise timing and tactical coordination; Most tasks are complex; Multi-modal tasks likely, requiring tight temporal coordination between modalities (concurrent or sequentially coupled)
	Flexibility	3 *(9)*	Adaptation likely to be required on moderate time scales (minutes to hours), during the operation
Aggregated Score		***-- (157)***	*Score for each level is 3x that of the next lower level in this example.*

Observations From These Examples

Scenario	Objective	Example Adversary Alternatives	Observations
High-Security Facility	Steal or Use Asset	• ??	Not observed – too difficult for expected gain?
Cyber Attack	Large $$ from Use of Info	• Few can generate a comparable return on investment	Attack *routinely* occurs
Large Truck Bomb	Destroy Building	• Burn down building	Alternative is easier for same consequences
	Mass Casualties	• Shootings in crowded areas • Suicide bomber vest • Car bomb in crowded area	Alternative is easier, but lower consequences



These factors are key inputs to the risk management method!

So, What Now?

Security emerges only as a system-level property.

Therefore, it can be managed only through effective systems engineering!

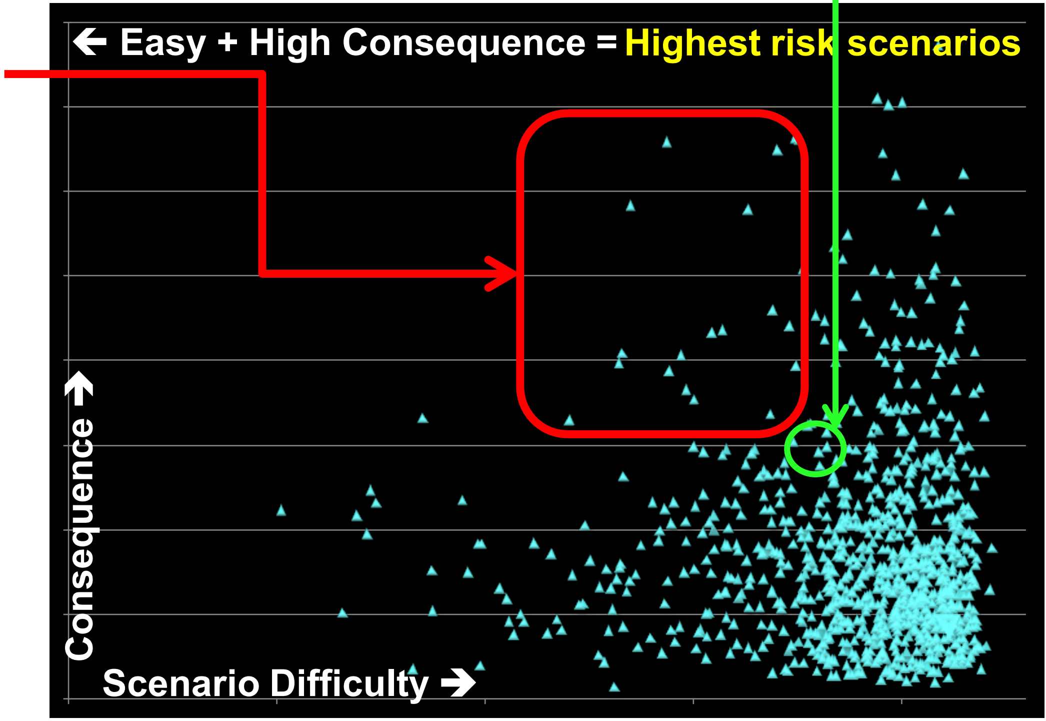
- The "security system" is just one part of the *complete* system
- "Vulnerabilities" often exist because of issues outside the "security system"
  - *Vulnerabilities and scenarios are often identified in an ad hoc manner*
- "Best practice" lists usually address only selected parts of the *complete* system

How can we manage security risk?

Sandia National Laboratories

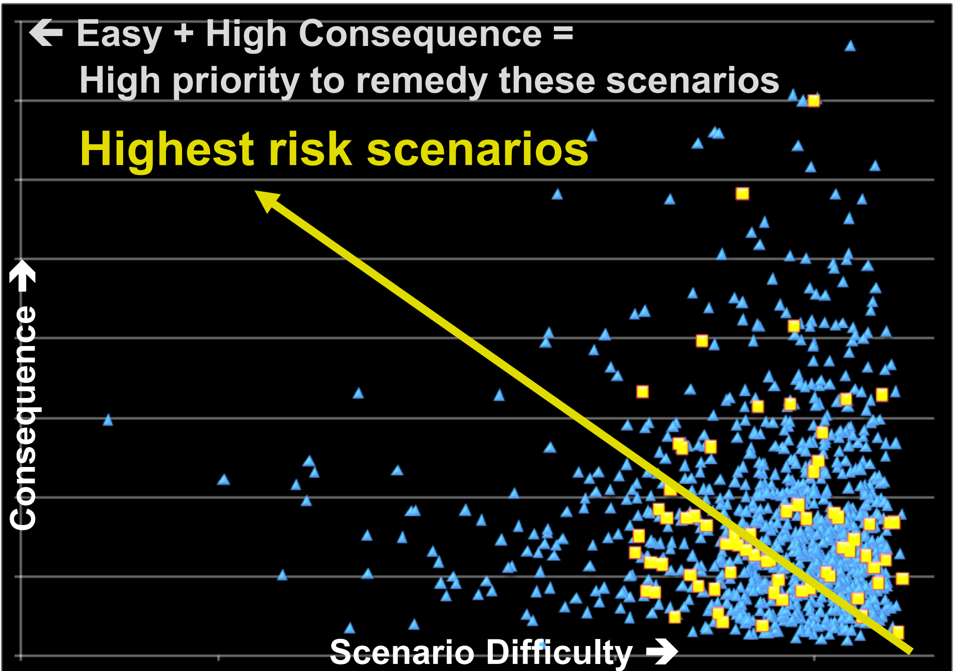
Practical Security Risk Management

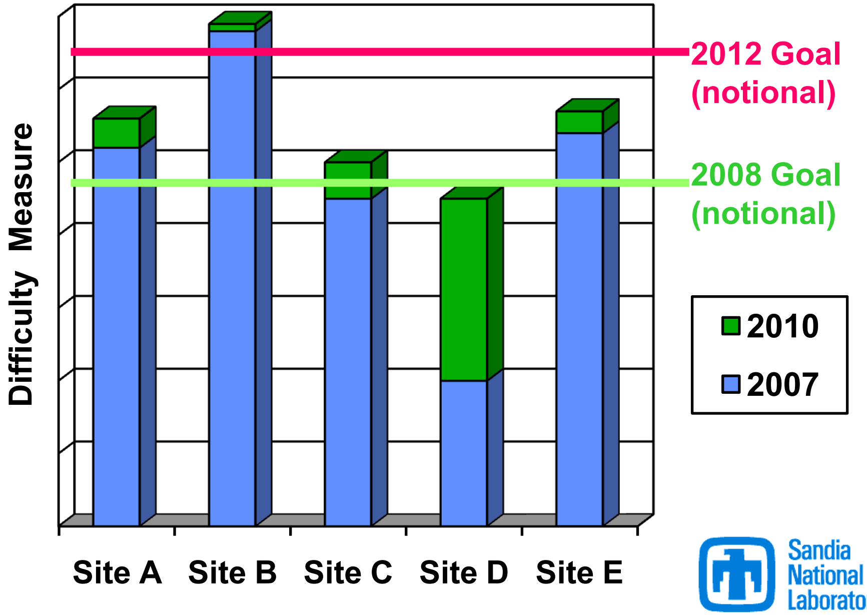
- Identify vulnerabilities or defeat methods
- Work these into scenarios that result in consequences
  - *Identify the expected consequences*
- Identify other easier ways for an adversary to generate comparable or greater consequences
  - *Initial security risk screening and prioritization*
- Use good systems engineering to find & rank mitigation options for higher risks
  - ↓ *consequence and/or* ↑ *difficulty*
- Continue throughout project lifecycle



Summary

- Focus on security risk *management*.
- Benefits of security investments can be inferred from two metrics:
  - How much harder has the scenario become for an adversary?
  - How much have expected consequences been reduced?
- Robust assessment of scenario difficulty is feasible.
- Method is scalable and encourages productive dialog among security professionals.


← Easy + High Consequence =
High priority to remedy these scenarios
Highest risk scenarios
Consequence →
Scenario Difficulty →


2012 Goal (notional)
2008 Goal (notional)
🟩 2010
🟦 2007
Difficulty Measure
Site A
Site B
Site C
Site D
Site E