SAND2006-6680C

Risk-Based Decision Approaches for Safeguards and Security Management

November 16, 2006

Presented by:

Gregory D. Wyss, Ph.D.

Distinguished Member of Technical Staff

Security Systems Analysis Department
Sandia National Laboratories

Co-Authors:

J. Darby, P. Dawson, K. Page and E. Ryder

Sandia is a multiprogram laboratory operated by Sandia Corporation, a Lockheed Martin Company,
for the United States Department of Energy's National Nuclear Security Administration
under contract DE-AC04-94AL85000.

Sandia National Laboratories

Overview

- Background and terminology
- Security system effectiveness
- Deterrence and pre-attack observables
- Considering consequences
- Last resort options
- Results and conclusions

Safety Risk vs. Security Risk

Safety	Security
• **Initiating event frequencies:**	
– *independent* events	– strongly *dependent* on both internal and external factors
– measurable or estimable	– if "measured" today, will likely be different tomorrow
• **Types of human actions:**	
– benevolent – assumed to be trying to resolve situation	– malevolent: working to defeat the system
– actions based on ignorance	– force, stealth, or deceit
• **Low frequency events…**	
– can be neglected	– can be ***caused*** to occur
• **Results for decision makers:**	
– roll up risk results into a single value or curve	– cannot "roll up" as initiating event freq's are unknown

Targets, Protection Strategies, and Design Basis Threats

- **Target: *What* is being protected**
  - **Item(s) or information**
  - **Theft, sabotage or misuse causes unacceptable consequences**

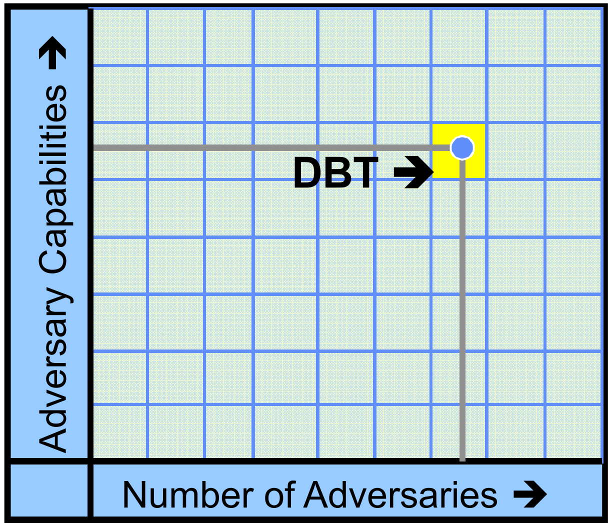
- **Design Basis Threat (DBT): What the target is being *protected against***
  - **How many adversaries?**
  - **Which weapons, tools, or other capabilities?**

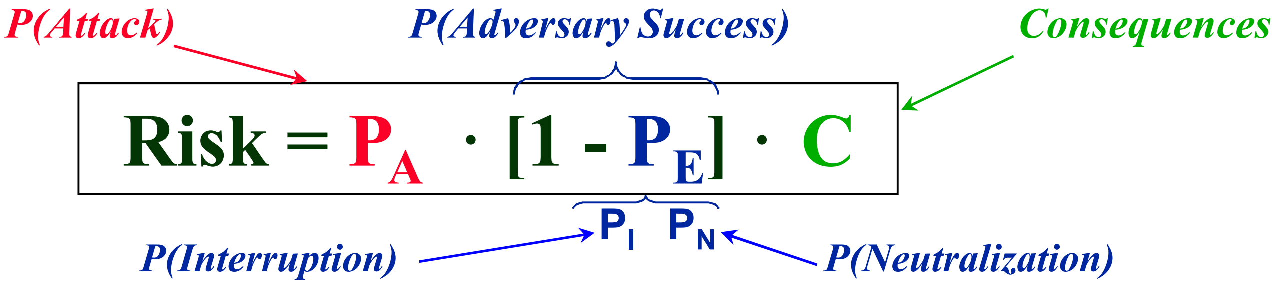
- **Protection Strategy: *How* it is to be protected**
  - **Deny access: simply touching or seeing the target is unacceptable**
  - **Deny task: must not let an adversary accomplish a specified task**
    - **Usually related to sabotage**
    - **Often: access for less than *n* hours or minutes**
  - **Deny theft: must not let the target leave the site**
    - **Containment is acceptable**

- **System Effectiveness (P_E): Probability that the security system is effective (i.e., the adversary is defeated) *if* a specific attack occurs**

Problem: Investment decisions based on only one aspect of risk

- **Issue: How can decision makers ensure consistent security investment decisions across its sites and targets?**
- **Problem: We have a dynamic security environment vs. a limited security budget**
  - **Perceived real-world threats have increased dramatically since 9/11/01**





P(Attack)

P(Adversary Success)

Consequences

$$\text{Risk} = P_A \cdot \overbrace{[1 - \underbrace{P_E}_{P_I \quad P_N}]} \cdot C$$

P(Interruption)

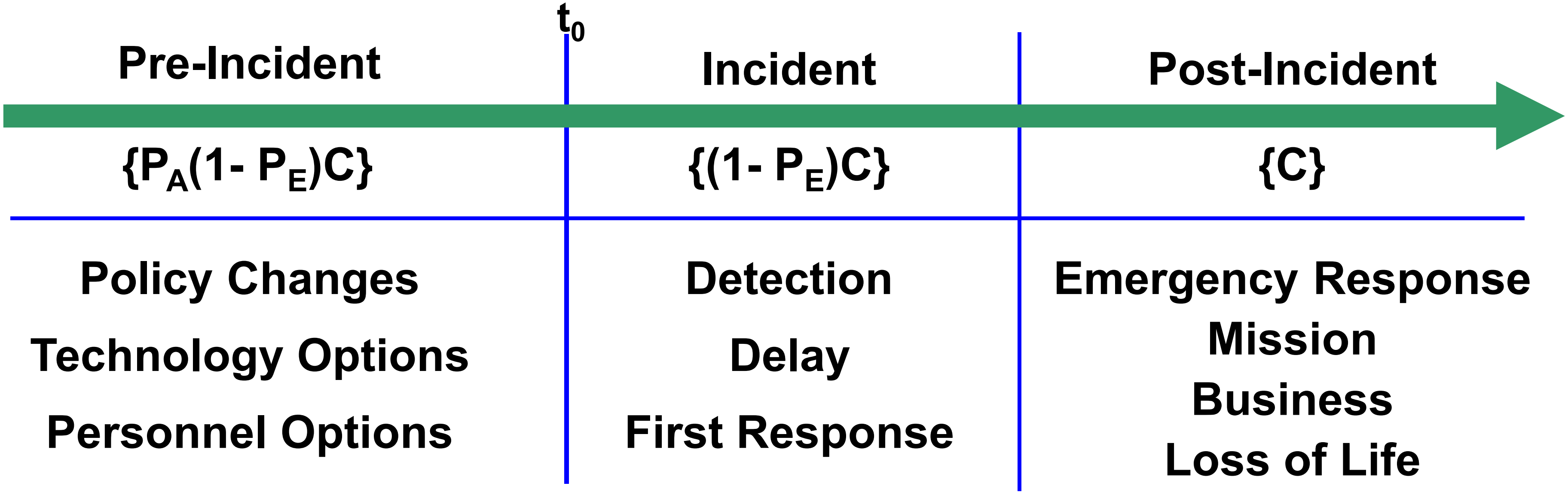
P(Neutralization)

- **To focus on P_E neglects important parts of the risk equation**
  - **May provide more cost-effective risk-reduction opportunities!**

Security Risk Equation and Timeline

$$\boxed{\text{Risk} = \overset{\textit{P(Attack)}}{P_A} \cdot \overbrace{[1 - \underbrace{P_E}_{P_I \quad P_N}]}^{\textit{P(Adversary Success)}} \cdot \overset{\textit{Consequences}}{C}}$$

P(Interruption) → P_I P_N ← *P(Neutralization)*

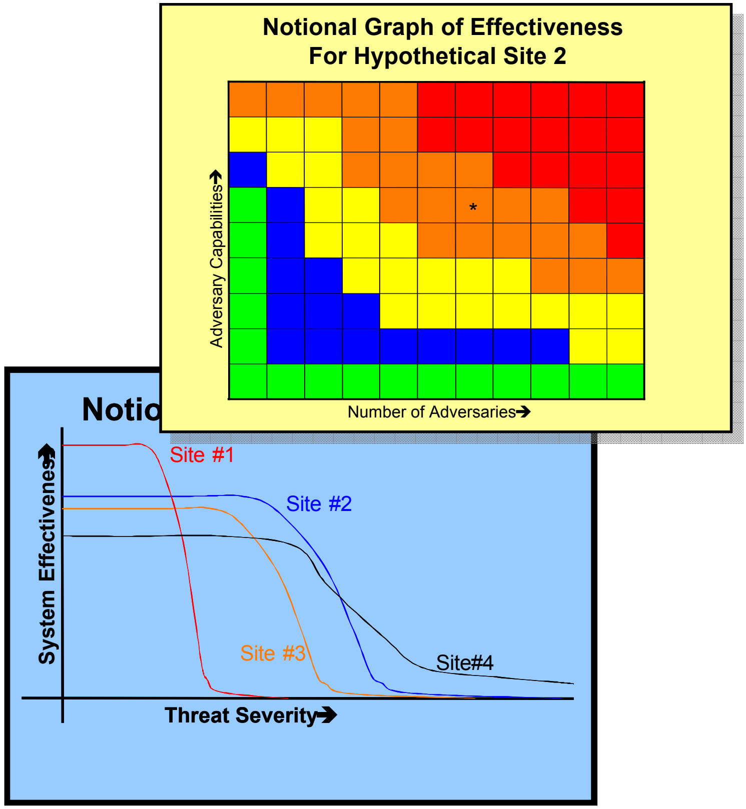


t_0

Pre-Incident	Incident	Post-Incident
$\{P_A(1- P_E)C\}$	$\{(1- P_E)C\}$	$\{C\}$
Policy Changes	Detection	Emergency Response
Technology Options	Delay	Mission
Personnel Options	First Response	Business
Planning Requirements		Loss of Life
		Costs
		Public Reaction
		Recovery

Risk-Based Decision Approaches

- Consider all parts of the risk equation to find ***differences*** between decision options
- Physical Security System Effectiveness
  - Use existing analyses and expert judgment to estimate P_E for a range of threats
    - Vary number & capability of adversaries, incl. beyond-design-basis threats
- Initiators: Look Beyond the Site Boundary
  - Qualitative look at the “layer of protection” beyond the site boundary
    - Examine differences in detection, interruption, and interdiction (e.g., topography, intelligence, interdiction by other agencies)



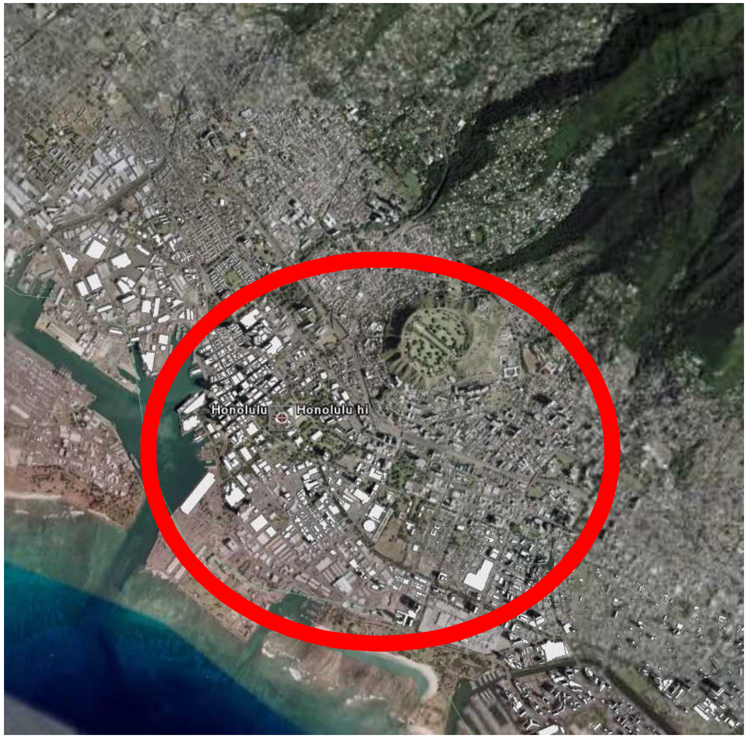
- Consequences: “On-site” scenarios vs. Theft scenarios
    - Examine differences based on both material and site characteristics
- Goal: a method to enable complex-wide security risk management

P_A: Observables to Law Enforcement

- **Transportation Sector**
  - **Unusual aircraft at local airports: easier to detect (site dependent)**
  - **“Typical” heavy equipment, trucks, etc.: harder to detect**
- **Local LEA**
  - **Facility surveillance**
  - **Local rehearsals**
  - **Local transportation**
  - **Presence of unusual people**
- **National LEA**
  - **Targeting**
  - **Weapon purchases & transfers**
  - **Attack scenario development**
- **International LEA**
  - **Global connections**
  - **Targeting**

Consequences

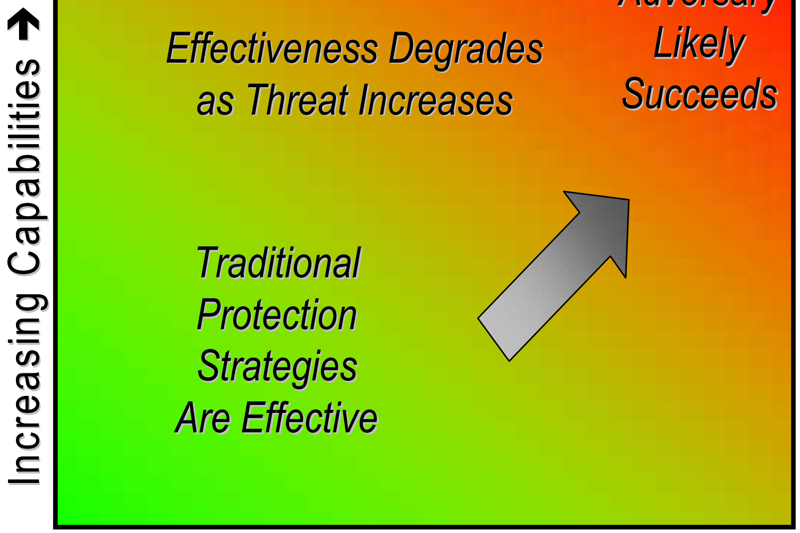
- **Consequences for theft are generally site-independent**
  - **Adversary chooses how and where to inflict consequences**
  - **Consequences depend on:**
    - **Characteristics of the theft target stolen**
    - **Goals and capabilities of adversary**
- **Consequences for on-site use are highly site-dependent**
  - **Sabotage scenarios**
  - **Consequences can *also* depend on:**
    - **Site characteristics**
    - **Topography, geography and population**
    - **Meteorology**
- **Differences in consequences may be large for some decisions but minimal for others.**



Nontraditional Security Investments

- Traditional security strategies:
  - Extreme adversaries can overwhelm security defenses
  - Perceived “real world” threats change frequently – often upward
  - Facility upgrades are long-term investments
- Is it possible to envision security systems that are effective against quasi-unbounded* threats?
  - Can we sacrifice function for security to protect against for the most extreme threats?

Protection Results

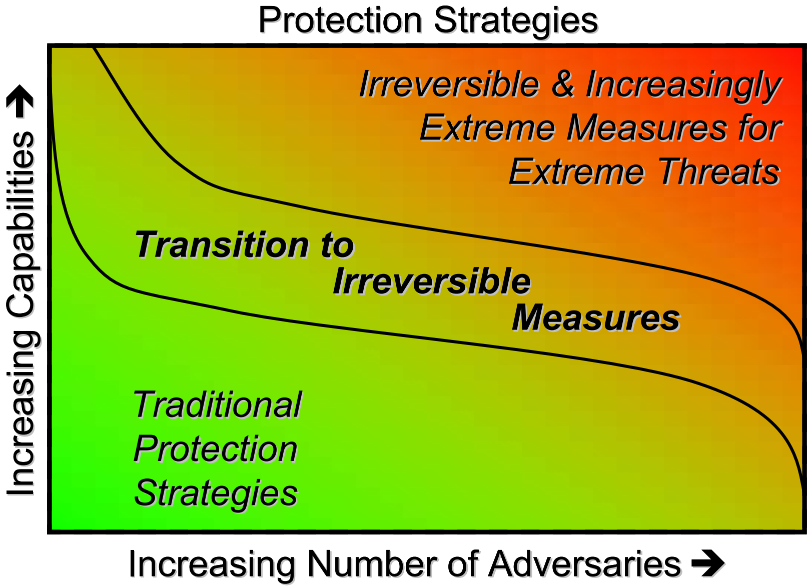

Increasing Capabilities ➔
Effectiveness Degrades as Threat Increases
Adversary Likely Succeeds
Traditional Protection Strategies Are Effective

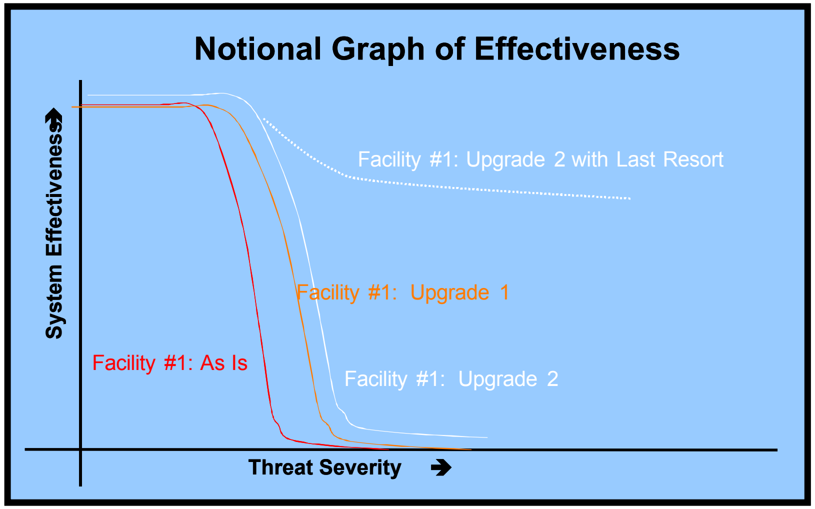
Increasing Number of Adversaries ➔

* Limited to “credible environments”

“Last Resort” Security Concepts

- **Last resort options can make a security system more robust**
  - **Trade functionality for ensured security at extreme threat levels**
  - **Graded responses to extreme threats**
- **Last resort options facilitate life-cycle cost and risk-based tradeoff studies**

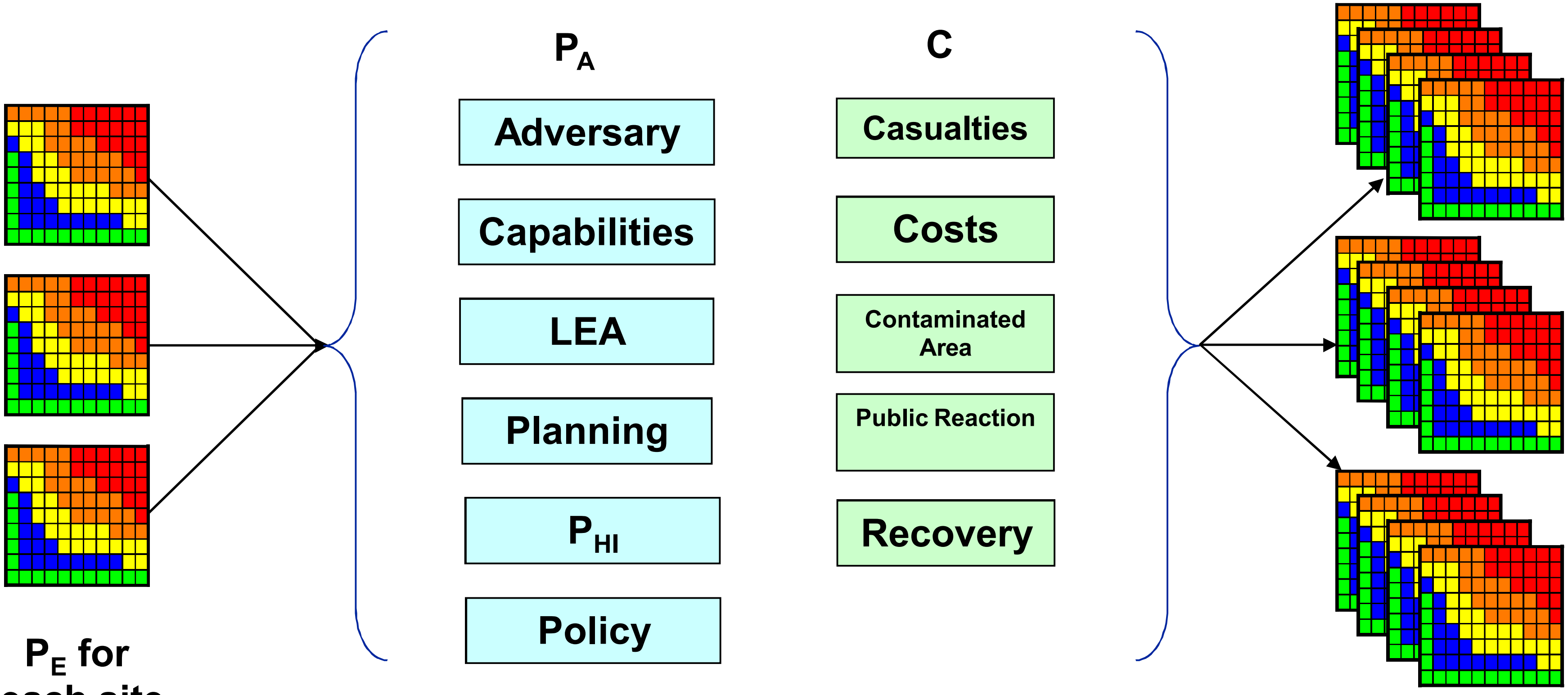

Protection Strategies
Irreversible & Increasingly Extreme Measures for Extreme Threats
Transition to Irreversible Measures
Traditional Protection Strategies
Increasing Capabilities →
Increasing Number of Adversaries →



- **Characteristics**
  - **Should be direct response to threat activities, if possible**
  - **~Irreversible – *<u>Nobody</u>* accesses or uses the facility or asset for an extended time**
  - **Requires redundancy to ensure facility or asset function continues to be met**
  - **Ensure against false activation**

Sandia National Laboratories

Risk Methodology



P_A

Adversary

Capabilities

LEA

Planning

P_{HI}

Policy

C

Casualties

Costs

Contaminated Area

Public Reaction

Recovery

P_E for each site

Risk for each site

Summary and Conclusions

- A risk-based decision approach to security analysis can help decision makers allocate scarce security resources.
- A method has been developed that:
  - Builds upon existing methods security analysis methods
  - Examines a range of threats
  - Uses all parts of the risk equation
- A pilot application has demonstrated this risk-based analysis method
- All parts of risk equation have an impact on risk
  - P_E has an impact on the potential for consequences
  - C will have an impact for some decisions
  - P_A allows more realistic scenarios
- Pilot gives confidence that complex-wide risk differences will be seen ***if*** analyses consistent across the complex