

Terrorism Risk Management for Critical Infrastructure Protection and Strategic Resource Allocation

Bryan S. Ware
CEO and Chief Scientist
Digital Sandbox, Inc.
www.dsbox.com
bware@dsbox.com



11/15/2005

2005 MORS Workshop on HLS/HLD
Copyright © 2005 Digital Sandbox, Inc.
www.dsbox.com

Overview

- The Terrorism Risk Management Challenge - What is Terrorism Risk?
- A Model Framework for Systematic Assessment and Management of Terrorism Risk
- Review of Legacy Risk and Vulnerability Assessment Processes that are Commonly used in HLS/HLD and Force Protection
- The Site Profiler® Terrorism Risk Management Framework

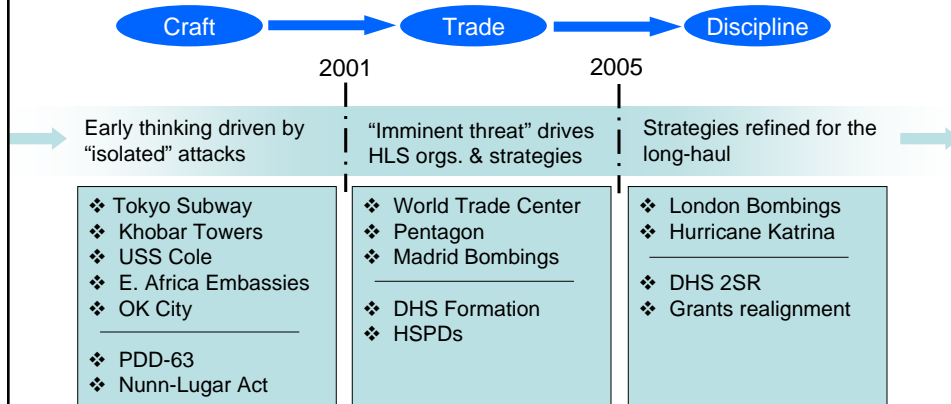


11/15/2005

2005 MORS Workshop on HLS/HLD
Copyright © 2005 Digital Sandbox, Inc.
www.dsbox.com

Terrorism and “Homeland Security”

Terrorism Risk Management: Only a decade old field, but rapidly maturing



11/15/2005

2005 MORS Workshop on HLS/HLD
Copyright © 2005 Digital Sandbox, Inc.
www.dsbox.com

Reaching the Next Level of Maturity

First, ask the right questions!!

- *What are my assets I should be protecting? Against what threats?*
- *What are my vulnerabilities and risks that I must address?*
- *How can I select the most cost effective risk mitigation measures?*
- *Given the scope of my challenge, how can I best obtain resources? How do I allocate the money and resources I do have?*

Apply controls, standards, and metrics

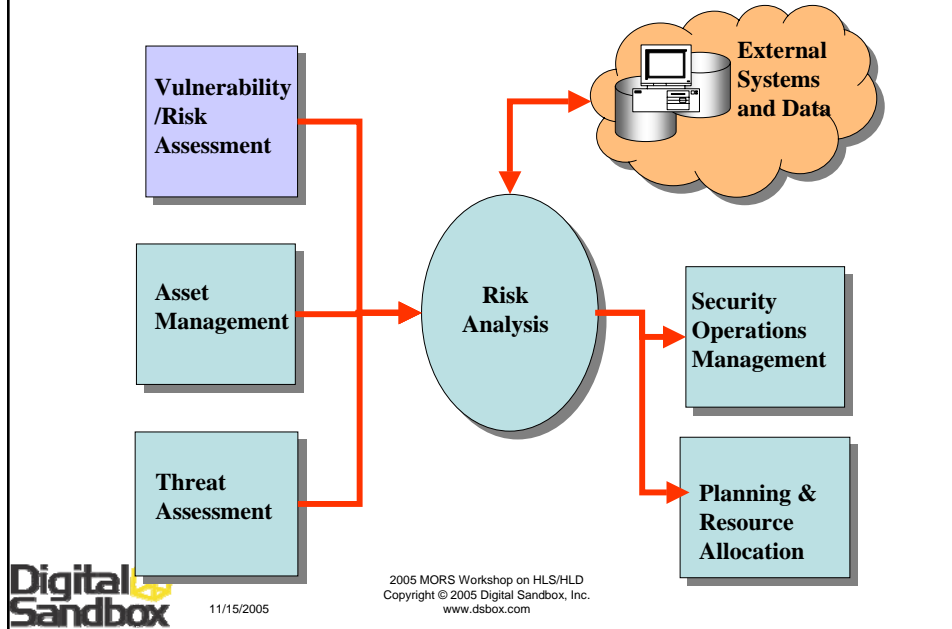
- *Risk analyzed dynamically, responsive to changing conditions*
- *Compiled results available on-demand to decision makers*
- *Key security, response, and resource allocation decisions driven by risk analysis*



11/15/2005

2005 MORS Workshop on HLS/HLD
Copyright © 2005 Digital Sandbox, Inc.
www.dsbox.com

A Systems Framework for Terrorism Risk Management



Review of Legacy Risk and Vulnerability Processes

Risk Processes, Methodologies, and Tools

- Risk Mnemonics
- Algebraic Expressions
- Fault Trees / Path Algorithms
- Simulations



11/15/2005

2005 MORS Workshop on HLS/HLD
Copyright © 2005 Digital Sandbox, Inc.
www.dsbox.com

CARVER

- CARVER is the risk/vulnerability process from which many variations have been derived
- Developed by US Special Forces circa Vietnam conflict
 - Used for targeting an adversary's installations
- Actually more of a *mnemonic* than a model
 - **C**riticality, **A**ccessibility, **R**ecognizability, **V**ulnerability, **E**ffect on the populous, **R**ecoverability
- CARVER has been misapplied to security applications, where it is intended to provide an "asset score". Originally trained as a thought process for highly trained operators, a numerical scale for each variable was developed so that it could be used by security personnel.



11/15/2005

2005 MORS Workshop on HLS/HLD
Copyright © 2005 Digital Sandbox, Inc.
www.dsbox.com

CARVER from an Analytical Perspective

- Each term in CARVER is evaluated on a 1 ⇒ 10 scale
- All variables are on a linear scale
- CARVER score is an unweighted sum
- Factors are excluded that do not fit the word (see also, CARVER2 or CARVER + Shock, etc.)
- All assets are alike: people, buildings, bridges all use the same “model”
- Unspecified pre-conditions and/or assumptions (how did you know it was an asset in the first place)
- Lack of dynamic range...no ability to rank or differentiate (60 - 6 = 54 bins)
- Combining orthogonal concepts and contexts: several risk terms in CARVER are known only in the context of a specific threat
- **Bottom Line:** Not suitable for prioritization of assets in large portfolios



11/15/2005

2005 MORS Workshop on HLS/HLD
Copyright © 2005 Digital Sandbox, Inc.
www.dsbox.com

Variants on the CARVER Theme

- Example Risk Mnemonics
 - CARVER2
 - used by DHS for the BZPP Program
 - CARVER + Shock
 - Used by FDA for food security
 - DSHARPP
 - Used by DoD
 - MSHARPP
 - Used by DoD and State & Local governments



11/15/2005

2005 MORS Workshop on HLS/HLD
Copyright © 2005 Digital Sandbox, Inc.
www.dsbox.com

Algebraic Expressions

- Often disguised as probabilistic expressions
- Most are of the general form:
 - Risk = Probability * Vulnerability * Consequences
- Many assume the Probability (threat term) to be 1
- Typically brittle expressions, with little ability to update or improve the equation
- Simplicity of use drives simple expressions that bely the complexity of the challenge

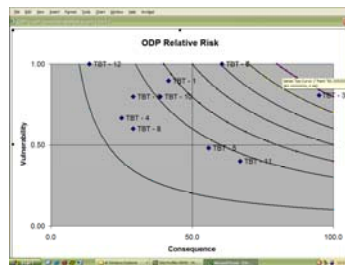


11/15/2005

2005 MORS Workshop on HLS/HLD
Copyright © 2005 Digital Sandbox, Inc.
www.dsbox.com

DHS Special Needs Jurisdiction Toolkit

- Typical use is for transportation agencies and port authorities to identify critical assets and assess unmet needs for risk reduction measures
- Used by DHS as the justification for grants
- Typically facilitated by subject matter experts



11/15/2005

2005 MORS Workshop on HLS/HLD
Copyright © 2005 Digital Sandbox, Inc.
www.dsbox.com

Other Algebraic Expressions

- Special Needs Jurisdiction Toolkit (SNJTK) and variants, MAST and TRAM
 - Developed, used, and required by DHS Office of Domestic Preparedness
- Analytical Risk Methodology (ARM)
 - Developed by CIA, used throughout the IC and State
- Strategic Threat and Risk Assessment (STAR)
 - Presented by DHS to the President
- Others
 - RAMCAP - Sponsored by DHS
 - FEMA 426
 - Mission Dependency Index (MDI) - NAVFAC and Coast Guard
 - PSRAT - Coast Guard



11/15/2005

2005 MORS Workshop on HLS/HLD
Copyright © 2005 Digital Sandbox, Inc.
www.dsbox.com

Fault Trees and Path Analysis

- These are systems that assume a threat baseline (often assuming that the probability of occurrence is 1) and use fault trees or paths to assess the vulnerability and often consequences for each given path
- Examples:
 - ASSESS: DOE program for Nuclear security
 - RAM - D: Sandia program for Dam security assessment
 - ERSM : Argonne program for event response assessment



11/15/2005

2005 MORS Workshop on HLS/HLD
Copyright © 2005 Digital Sandbox, Inc.
www.dsbox.com

Simulations

- Simulations, particularly of complex interdependent infrastructures, are used to enable risk based decision support
- The focus is typically on the system vulnerabilities of the infrastructure and the cascading consequences of an event
- These systems typically have intense data needs that may limit their use and require substantial expertise and computer resources
- Examples:
 - CIP-DSS: DHS Science & Technology program
 - FortiusOne: Commercial product in use at DHS



11/15/2005

2005 MORS Workshop on HLS/HLD
Copyright © 2005 Digital Sandbox, Inc.
www.dsbox.com

The Site Profiler® Terrorism Risk Management Framework



11/15/2005

2005 MORS Workshop on HLS/HLD
Copyright © 2005 Digital Sandbox, Inc.
www.dsbox.com

Answering the Right Questions

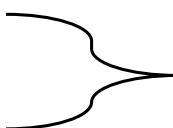
- The questions we must answer:
 - *What are my assets I should be protecting? Against what threats?*
 - *What are my vulnerabilities and risks that I must address?*
 - *How can I select the most cost effective risk mitigation measures?*
 - *Given the scope of my challenge, how can I best obtain resources? How do I allocate the money and resources I do have?*
- Expanding on the legacy systems and approaches
 - Many legacy approaches are far too simple to support analytical purposes
 - Several of the more sophisticated approaches provide only a single component of risk, without presenting the whole picture, and may require significant resources (including time) to facilitate decisions
- Terrorism Risk Management requires a systematic analytical framework to support effective decision making



11/15/2005

2005 MORS Workshop on HLS/HLD
Copyright © 2005 Digital Sandbox, Inc.
www.dsbox.com

Probability Continuum

- Impossible
 - Possible
 - Plausible
 - Likely
 - Probable
 - Certain
- 
- Our work focuses in this region*

Our methodology seeks to provide a structure and metrics for prioritizing events for which there is high uncertainty and little history.



11/15/2005

2005 MORS Workshop on HLS/HLD
Copyright © 2005 Digital Sandbox, Inc.
www.dsbox.com

A Framework for Modeling Terrorist Risk

- The Focus Is to Efficiently Allocate Resources Across Known, Historical Security Issues and Potentially High Consequence Future Events
- Prioritization of Assets: *Criticality, Desirability, Accessibility*
- Prediction of Future Events: *Time, Weapons, Tactics, Organizations*
- Assessment of the Consequences of Those Events
- Development and Stress Testing of Risk Mitigation Strategies



11/15/2005

2005 MORS Workshop on HLS/HLD
Copyright © 2005 Digital Sandbox, Inc.
www.dsbox.com

Methodology (Rationale)

- Complex decisions are made by breaking problems down into smaller chunks that are more readily understood and bounded. Experts, anecdotal evidence, simulations, and even data are available when the chunks are small enough.
- Strategic and value decisions are made by considering cognitive or domain relationships (Aristotle's "Concept") which are unique to each individual and may have complex dependencies and structure.
- The physical world (Aristotle's "Substance") can be readily and unambiguously described through inheritance. Understanding of the physical world is necessary for detailed and tactical decision making and the assessment of physical phenomenology.



11/15/2005

2005 MORS Workshop on HLS/HLD
Copyright © 2005 Digital Sandbox, Inc.
www.dsbox.com

The General Approach

- Bayesian Risk Metrics Represent the Degree of Belief That a Threat is Plausible, for example. (*vs. a frequentist approach that represents the ratio of events to non-events*)
- Analytic Foundation is Dynamic, Object-Oriented Bayesian Networks
 - Substance: World Object Model
 - Concept: Domain Object Model
 - Drivers: Composable Risk Influence Networks (RIN)
- The Domain Model and RIN Implicitly Represent Causality
- Expert Judgment Is Used Where Appropriate (And Essential)
- Risk = f (Likelihood, Susceptibility, Consequences)



11/15/2005

2005 MORS Workshop on HLS/HLD
Copyright © 2005 Digital Sandbox, Inc.
www.dsbox.com

Observations and Conclusions

- Certain Events Are Not Amenable to Traditional Methods
 - Methods that represent a combination of data and expert judgment are key to understanding
- Modeling of Causality Provides Insight into Risk Drivers and Correlation
 - Enables true *enterprise* risk management programs
- Traditional Scenario Modeling and Worst Case Modeling May Provide Misleading Results
 - Ensure that scenarios don't represent a pre-filter on possibilities and that second (and nth) order effects are considered in loss calculations



11/15/2005

2005 MORS Workshop on HLS/HLD
Copyright © 2005 Digital Sandbox, Inc.
www.dsbox.com

Back-up Overview of Simple Bayesian Network and Software/System Description



11/15/2005

2005 MORS Workshop on HLS/HLD
Copyright © 2005 Digital Sandbox, Inc.
www.dsbox.com

Bayesian Network Basics

Conditional Probability

$P(A | B) = X \Rightarrow$ Given the event B, the Probability of A is X

Bayes Rule

$P(B | A) = \frac{P(A | B) P(B)}{P(A)} \Rightarrow$ The Probability of B given A is equal to the Probability of A given B times the Probability of B, divided by the Probability of A

Parameters of Interest and States

A = The chance of rain
States = High (a_1), Medium (a_2), Low (a_3)
B = The chance you'll carry an umbrella
States = High (b_1), Medium (b_2), Low (b_3)

Conditional Probability Table

	b_1	b_2	b_3
a_1	0.8	0.15	0.05
a_2	0.2	0.6	0.2
a_3	0.1	0.2	0.7



11/15/2005

2005 MORS Workshop on HLS/HLD
Copyright © 2005 Digital Sandbox, Inc.
www.dsbox.com

Differentiators

Foundational Risk Methodology – comprehensive and extensible

Risk Methodology

Analytic Method

RIN analytics – Dynamic and scalable

Site Profiler Enterprise System – Proven in operational environments

Deployable System

Concept of Operations

Only firm to integrate systems with people and processes



11/15/2005

2005 MORS Workshop on HLS/HLD
Copyright © 2005 Digital Sandbox, Inc.
www.dsbox.com

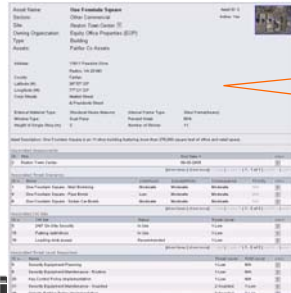
Site Profiler Product Line



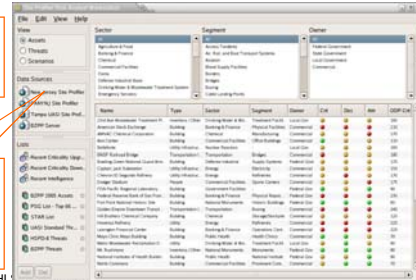
Assessor Field Tool



3D Blast Modeling Tool



Enterprise Server



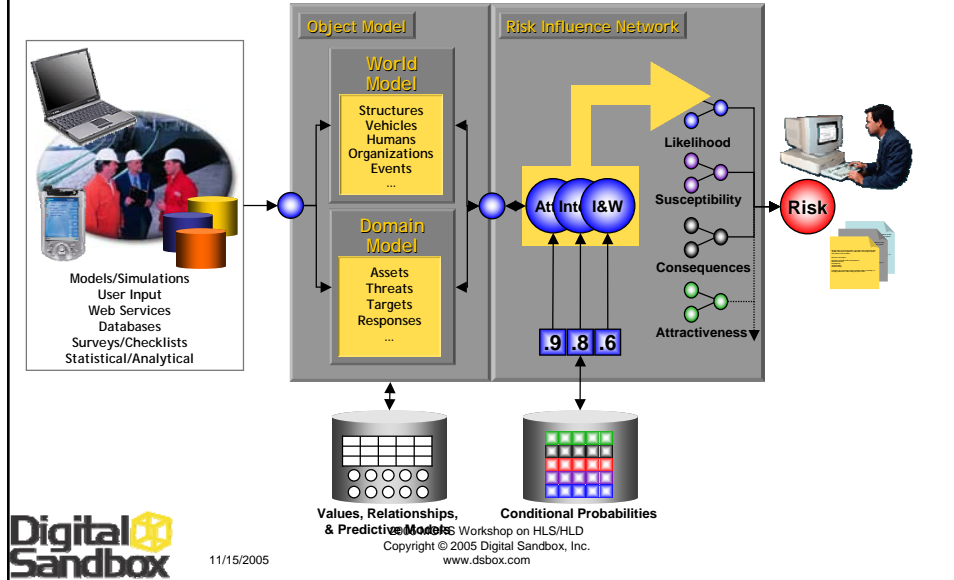
Risk Analysis Workstation



11/15/2005

2005 MORS Workshop on HLS/HLD
Copyright © 2005 Digital Sandbox, Inc.
www.dsbox.com

How it Works



Patent Pending Risk Analytics

