2011

Delayed-Bang Approach Towards More Sustainable Critical Infrastructure Risk Management

C. Ariel Pinto
Old Dominion University, cpinto@odu.edu

Michael K. McShane
Old Dominion University, mmcshane@odu.edu

Abhishek S. Pathak
Old Dominion University

Original Publication Citation

Pinto, C.A., McShane, M.K., & Pathak, A.S. (2011). Delayed-bang approach towards more sustainable critical infrastructure risk management. *Journal of Homeland Security and Emergency Management, 8*(1), 1-15. doi: 10.2202/1547-7355.1533

Journal of Homeland Security and Emergency Management

Volume 8, *Issue* 1 2011 *Article* 23

Delayed-Bang Approach Towards More Sustainable Critical Infrastructure Risk Management

C. Ariel Pinto, *Old Dominion University*
Michael K. McShane, *Old Dominion University*
Abhishek S. Pathak, *Old Dominion University*

Recommended Citation:
Pinto, C. Ariel; McShane, Michael K.; and Pathak, Abhishek S. (2011) "Delayed-Bang Approach Towards More Sustainable Critical Infrastructure Risk Management," *Journal of Homeland Security and Emergency Management*: Vol. 8: Iss. 1, Article 23.
DOI: 10.2202/1547-7355.1533

Delayed-Bang Approach Towards More Sustainable Critical Infrastructure Risk Management

C. Ariel Pinto, Michael K. McShane, and Abhishek S. Pathak

Abstract

This article describes the Delayed Bang Approach for determining the value of risk management alternatives in critical infrastructure security. The discussion includes (1) the need for sustainable risk management (2) the importance of time valuation in evaluating competing loss prevention and loss reduction alternatives, (3) the convergence of deterministic engineering economics, survivability analysis , and probabilistic analysis, and (4) hypothetical examples of the Delayed-Bang Approach and significance towards more sustainable risk management.

KEYWORDS: risk management, critical infrastructure, security, engineering economy, cost-benefit analysis

Author Notes: The authors would like to acknowledge Old Dominion University Department of Engineering Management and Systems Engineering, ODU Office of Research Collaborative Research Seed Grant, and the Emergent Risk Initiative at ODU for their support in this research project.

Introduction

"An ounce of Prevention is worth a pound of cure" - Benjamin Franklin (1706 - 1790). In the present day scenario of U.S. critical infrastructure security, one may ask if Benjamin Franklin's words can provide guidance and confidence on how decision makers and policy makers of this country treat *loss prevention* and *loss reduction* (i.e. cure) from security disruptions. Unfortunately, there is still no generally accepted way to determine how much loss prevention is worth relative to loss reduction (Pinto and Pathak, 2008). In this paper, we introduce the Delayed Bang Approach, which draws on engineering economics, survivability analysis, and probability theory for evaluating the value of loss prevention and loss reduction alternatives.

The premise of this article is analogous to Benjamin Franklin's allusion. The security of critical infrastructures is being dealt with by a combination of strategies to prevent security incidences from happening, and to reduce losses when such incidents do happen. We use definitions commonly found in descriptions of the risk management process. "Loss prevention refers to measures that reduce the frequency of a particular loss" and "loss reduction refers to measures that reduce the severity of a loss after it occurs" (Rejda, 2011, p. 48). For critical infrastructure security, an example of loss prevention is deployment of radiation detectors to lessen the chance of a dirty bomb entering the country through its ports. An example of loss reduction is the preparation of evacuation plans of port employees, just in case a dirty bomb is not detected early enough and exploded inside the port.

Arora, et al. (2004) have emphasized that there is no cure-all when it comes to security, and that aside from the fact that everyone wants more security, it is not clear "how much to spend for this added security" (p.1). Arora, et al. further observed the lack of "structured cost-benefit methods to evaluate" risk management alternatives, essentially resulting in an ad hoc resource allocation in risk management (p. 2). For organizations, risk management activities do not produce revenue but rather are cost-centers that provide essential and necessary support for the overall mission of the organization. As such, the relevant criterion in evaluating risk management resource allocation in critical infrastructure security is not simply the cost of implementation, which everyone agrees need to be minimized, but rather how much incremental benefit each additional dollar of "investment" brings, in the form of reducing the expected loss or risk.

For example, maritime ports, similar to most other critical infrastructures, are privately owned and operated as a profit-seeking firm. Since 9/11, the port operators have been tasked by the federal government to attain a certain level of security. Being in a very competitive industry, port operators need to be aware of how security related activities will affect their cost, efficiency of operation, and

eventually capacity to compete with other ports. The same can be said about other organizations and how they deal with security, whether it is other types of transportation systems operators, or even universities.

This article discusses a new and novel approach – termed the Delayed Bang Approach – to aid security risk analysts and decision makers in valuing and choosing among alternatives by describing these alternatives in terms of two dimensions: (i) loss prevention and (ii) loss reduction. This approach, an amalgamation of risk management, survivability analysis, and engineering economy, is meant to capitalize on trends towards more sophisticated data analysis and data fusion tools and shifts in local and national security-related policies.

Challenges in Valuing Loss Prevention and Loss Reduction

There are several reasons why researchers and practitioners are struggling at valuing the worth of risk management resources. These can be discussed under two topics: (1) the differences between risk-based benefits and traditional benefits, and (2) the security-probability dilemma.

Risk-based benefits can be described as either loss prevention, that is, the reduction in the chance of a risky event occurring or loss reduction, meaning the reduction in consequence if the event does occur. In both cases, the benefits do not come in the traditional form: the former is an abstract concept of chance commonly expressed as a ratio, a fraction or decimal number between zero and one; and the latter is a conditional benefit that may come in terms of monetary value, but is still conditioned by chance. Statistical expected value can be used to numerically reconcile this problem, but may not totally apply to critical infrastructure protection where some risky events have potentially large consequences and small probabilities. It is noteworthy that this benefit does not necessarily translate into additional resources, which companies would typically use for other productive endeavors. Thus, risk-based benefits cannot simply be treated as traditional benefits in most analysis because the assumption of re-investment is not valid (Arora, et al., 2004).

What is the security-probability dilemma? One metric of a more effective security risk management is the reduction in the chance of occurrence of the security event. However, this reduction in the chance of occurrence is complicated by the interaction between those responsible for security measures and those trying to overcome the security measures. The threats to security (i.e. the bad guys) are often persons or organizations that gather information and form strategies to overcome all security barriers that we (the good guys) put in place to stop them. This is the primary reason secrecy and covertness plays such an important role in security risk management - akin to any game of strategy like

chess or poker where players would like to capitalize on asymmetric information. As such, the real chance of occurrence of a security event becomes more uncertain. In essence, the more sophisticated the security game becomes and the better the players are in playing this game, the more uncertainty there is surrounding the real effectiveness of loss prevention and loss reduction activities.

In addition, the consequence of a security event is not independent of its likelihood. Being similar to a game of strategy – the consequence is similar to a payoff for the bad guys. As such, the higher the consequence (i.e. high payoff), the more attractive it is for the bad guys. Yezer (2005) aptly described this situation where "even if the average return to terrorism is not large, there are some cases of spectacular rewards."

In response, previous research presented a framework such that benefit is based on avoided risk rather than more traditional increased productivity. One is in the form of Risk-based Return-on-Investment (RROI), a modified ROI. However, RROI only indicates when to stop investing in security, and not the more important task of choosing between alternatives.

Risk Management, Survivability Analysis, and Engineering Economics

Our focus on loss prevention and loss reduction is rooted in the definition of risk. Risk can be described quantitatively as a joint function of the likelihood of undesirable events and their consequences. That is,

Risk =f (likelihood, consequence) (1)

The primary objective of risk management is to reduce risks. However, just like any other engineering management activity, the reduction in risk has to be balanced with associated costs. Nonetheless, recent national and international economic turmoil have led policy and decision makers to implement fiscal conservatism in spending for risk management activities. This situation creates a challenging environment for continuous and consistent (i.e. sustainable) management of risks. This is especially true for engineering endeavors that have particularly high technological content such as software development and maintenance and network infrastructure development (Pinto, Arora, Hall, and Schmitz, 2006).

Considering loss prevention and loss reduction, it is essential that alternative actions be evaluated based on their costs and benefits, where the benefits naturally will be based on the potential for reduction in risks. Accordingly, the risk of any scenario can be reduced by reducing the consequence associated with the scenario, or reducing the likelihood of occurrence, or both.

However, benefit measured in terms of reduction in risk is not the same as benefit measured in terms of profit.

There is also difficulty in accurately estimating the consequence and the likelihood functions associated with a risk scenario. This can be due to the lack of *apriori* information for projects that are unique, such as projects at the forefront of technology, or that involve highly reliable systems for which there are very few historical records on which risk assessment can be based, such as critical infrastructures (Haimes, 1998).

Obviously, critical infrastructure security is an area very akin to risk management. A related topic to risk is *survivability analysis,* which deals with the death of biological organisms and failure of mechanical systems. It is also called reliability theory or reliability analysis in engineering, and duration analysis or duration modeling in economics or sociology (Johnson and Johnson, 1999). An important aspect in survivability analysis that is relevant to critical infrastructure security is the extensive modeling of time to event data (the survival function), conventionally denoted S, which is defined as

$$S(t) = Pr(T > t) \qquad (2)$$

Where t is time, T is a random variable denoting the time-to-event, and "Pr" stands for probability. That is: the survival function is the probability that the time-to-event is later than some specified time. Survival function or survivorship function is the term used in problems of biological survival whereas reliability function is used for mechanical survival problems. In the context of risk management, the occurrence of the risky event is considered an "event" in survivability analysis literature. Survivability analysis attempts to answer questions such as how do particular circumstances or characteristics increase or decrease the odds of survival (Colette, 2003).

Engineering economics is the application of economics to engineering projects. Engineers try to find solutions to problems, and the economics of each probable solution is considered along with the technical aspects. Costs as well as revenues are considered for each alternative for an analysis period that is either a fixed number of years or the estimated life of the project.

Time value of money is one of the most important concepts in engineering economics. The common notion in time-valuation of money (or resources in general) is that resources that the firm has in its possession today are more valuable than resources in the future because these resources can be invested and directly put into productive activities and earn positive returns. Engineering managers are always presented with opportunities to earn positive rates of return on their resources via attractive engineering projects. Therefore, the timing of

cash outflows and inflows has important economic consequences, which engineering managers clearly recognize as the "time value of money".

A time line is often used to depict the cash flows associated with a given investment. It is a horizontal line on which time zero appears at left most end when the investment is made and future periods are marked to the right. Because money has time value, all of the cash flows associated with an investment must be measured at same point in time. Generally, the present value is calculated for the investment cashflows at the appropriate discount rate, then the cost of the investment is subtracted. The investment should be made if the net present value (NPV) is positive.

Delayed Bang Approach

The Delayed Bang Approach is a theoretical method developed to estimate the value of critical infrastructure loss prevention and loss reduction alternatives by visually representing their costs and benefits on a timeline together with other events that may affect or result from these alternatives. The precept of this approach is that resources available to secure critical infrastructures are scare, and to paraphrase Benjamin Franklin's famous proverb, there is a tradeoff between loss prevention and loss reduction. The Delayed-Bang Approach is based on the following axioms.

Axiom 1: Risk management resources can be described in terms of their effects on loss prevention and loss reduction.

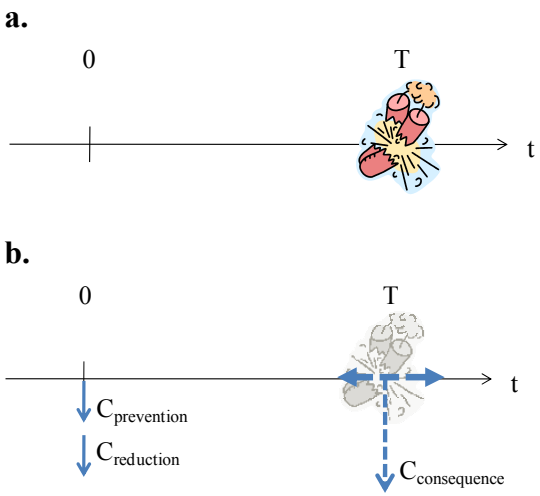
Axiom 2: The likelihood of a risky event can be expressed as time-to-event.

Axiom 3: For certain types of risky events (e.g. mechanical failure, security events), the natural tendency is always for the risky event to occur sooner if no effort is made for loss prevention.

Recall the notion of risk as a function of likelihood and consequence in Equation 1. This notion reinforces the two dimensions of critical infrastructure security—loss prevention and loss reduction—mentioned in Axiom 1, which deal with likelihood and consequence respectively. The inherent challenge of estimating and expressing the likelihood of risky events is dealt with by Axiom 2, which recognizes that there are ways to estimate and express such uncertainty, commonly known as subjective probability. The Delayed Bang Approach treats subjective probability similar to the concept of time-to-event in survivability analysis (as described in the previous section) because the primary interest is the next occurrence, and not the long-term rate of occurrence of a security event.

Exhibit 1 graphically presents a horizontal timeline with a vertical line that marks the present. A risky event that has not happened yet is graphically represented by the explosion. The time from the present up to the estimated occurrence of the risky event is represented by the time-to-event T (Exhibit 1a).

Exhibit 1. Delayed Bang Approach (a) using time-to-event T and (b) changes toT and consequence.



Definition 1: Loss prevention pertains to an act that pushes the occurrence of the risky event further into the future.

This definition is partly derived from the general notion of prevention as well as from Axiom 2. This allows the effective use of a timeline to show the effect of efforts to prevent a risky event, essentially increasing the estimated time-to-event T.

Definition 2: Loss reduction pertains to an act that reduces the consequence of the risky event if it does occur.

And since the primary interest is the next occurrence, and not the long-term rate of occurrence of the risky events, the effectiveness of loss prevention and loss reduction can be judged solely on their effect on the next event. This leads to the fourth axiom.

Axiom 4: Loss prevention and loss reduction are meant to affect the next occurrence of the security event, and not subsequent occurrences.

The fourth axiom is consistent with the common notion of extreme, rare, and catastrophic events, where a single occurrence can change the environment drastically such that much of the pre-event analyses do not apply post-event. Exhibit 1b shows a simplified case of how the likelihood of a security event and the consequence, if it occurs, can be represented on a timeline together with the costs of loss prevention and reduction. This figure shows the costs of loss prevention and reduction as two downward pointing arrows at the present time, representing the out-flow of resources. The figure also shows how these costs affect how far in the future the security event will occur and also changes to the consequence, represented by the dashed horizontal and vertical arrows respectively.

In essence, the Delayed Bang Approach combines traditional cost-benefit analysis with loss estimation (e.g. Rose, et al., 2007) in the area of crime prevention (e.g. Chisholm, 2000) with recognition of the ever-evolving technologies in data mining, security intelligence, data fusion, and probabilistic terrorism risk modeling (e.g. Willis and LaTourette 2008).

Although the Delayed Bang Approach may be a relatively new approach, the activities comprising the approach are nonetheless consistent with traditional risk assessment, modeling, and management. It can be noted that the generally acceptable risk management framework (i.e. Six Questions in Risk Management) described by Haimes (1998) is consistent with those of the Delayed Bang approach, as shown in Exhibit 2.

Exhibit 2. Correspondence between the Delayed-Bang Approach and the General Risk Management Framework.

Six Questions in Risk Management	**Equivalence in Delayed Bang Approach**
1. What can go wrong?	Identification of the security event scenario
2. What is the chance of occurrence?	Estimation of time-to-event T
3. What are the consequences?	Estimation of the consequences if the event does occur
4. What are the alternatives?	Identification and description of loss prevention and loss reduction alternatives
5. What are the tradeoffs?	Cost and benefit analysis
6. What are the effects on future decisions?	Resource allocation and iteration.

In the realm of theoretical research, this approach addresses the central issue of balancing marginal benefits and costs for the purpose of policy making, a recognized area of needed research. Additionally, this approach will provide practitioners in risk management the advantages of structured cost-benefit analysis, whereby:

- Security managers make their assumptions explicit and capture decision rationale.
- Security-related decisions are re-evaluated consistently when assumptions change.
- Security managers see whether investment is consistent with risk expectations.

Method

The method for applying the Delayed Bang Approach suits the framework described in Exhibit 2. The method entails six steps as described below.

Step 1 - Identification of the security event scenario. This step involves the identification and description of a particular security event scenario deemed by the risk analyst to be of critical importance to decision makers and the system at hand. It should be emphasized that since the Delayed Bang Approach adapts concepts from survivability analysis, the security events suitable for this method are those whose next occurrence is more important than subsequent occurrences.

Step 2 – Estimation of time-to-event (T). The time-to-event pertains to the estimate of when the next occurrence of the security event will occur. Recognizing the high degree of uncertainty of this estimate, the analyst should prudently choose the proper method or technique for estimation.

Step 3 – Estimation of consequences if the event occurs (C). Estimating the consequences, though also subject to a high level of uncertainty, is essentially an analysis of the asset being protected, and as such is similar to traditional cost and consequence estimation techniques. Several recent methods are available for estimating the consequence of a security events, such as Input-Output Analysis (Cheng, et al. 2006), supply/demand-side economic simulation (Park, 2008), and systematic (full impact) economic estimation using off-the-shelf software (Lee, et al. 2008), among others.

Step 4 – Identification and description of loss prevention and loss reduction alternatives. This step involves not only the enumeration of alternatives (e.g. technologies, policies, etc.) that are considered to have the potential to reduce the risk of the earlier identified security event scenario, but also the detailed description of their initial and ongoing costs and impact of loss prevention (i.e. reduction in the time-to-event T) and the impact of loss reduction if the event occurs (i.e. reduction in the consequence C).

Step 5 – Cost and benefit analysis. This step is essentially an evaluation of the time-valued costs and benefits of the risk management alternatives identified and described in the preceding step. There can be at least two ways of evaluating the alternatives. One way is by comparing them with each other and the other is by comparing them with the do-nothing alternative. An important piece of information in this analysis of the alternatives is the discount rate to be used, which can be the same discount rate that would have been used if these were the more traditional engineering endeavors (e.g. choosing between investment portfolios, machines, etc.)

Step 6 – Resource allocation and iteration. After the analyst has performed the cost and benefit analysis and presented the results, the decision makers may then use these results in conjunction with other information to arrive at a particular strategy of investing in none, one, or a number of the alternatives. Recognizing the highly dynamic nature of security risk management, the analyst needs to update the results based on new information which may significantly affect the initial analysis results.

Example Hypothetical Applications

Example 1A – 1st Generation sensor technology with unknown time-to-event T. The US Custom Border Patrol is planning to deploy a new unmanned remote radiation sensor at a US border point to prevent the entry of dirty bombs which can cause an estimated $200M in damage. This event is believed likely to occur as early as 5 years from now if no intervention is done. How effective should this plan be in preventing such an event to make it cost-justified?

Step 1 - Identification of the security event scenario. For this particular example, the security event can be described as “the entry of a dirty bomb at a particular point of entry and its eventual detonation.”

Steps 2 & 3 – Estimation of time-to-event (T) and consequences (C). From the narrative of this example, the time-to-event (T) and consequences (C) are 5 years and $200M, respectively, in the case of doing nothing.

Step 4 – Identification of alternatives. This particular example presents two alternatives: a new unmanned remote radiation sensor and do-nothing. Pertinent information is shown in the first three columns of Exhibit 3.

These are

- Initial set up cost for infrastructure and technology acquisition
- Yearly cost that includes operation and maintenance
- Discount rate used to discount future cash flows to their present values, which usually represents the acceptable rate of return for investment
- Time-to-event T
- Consequence C

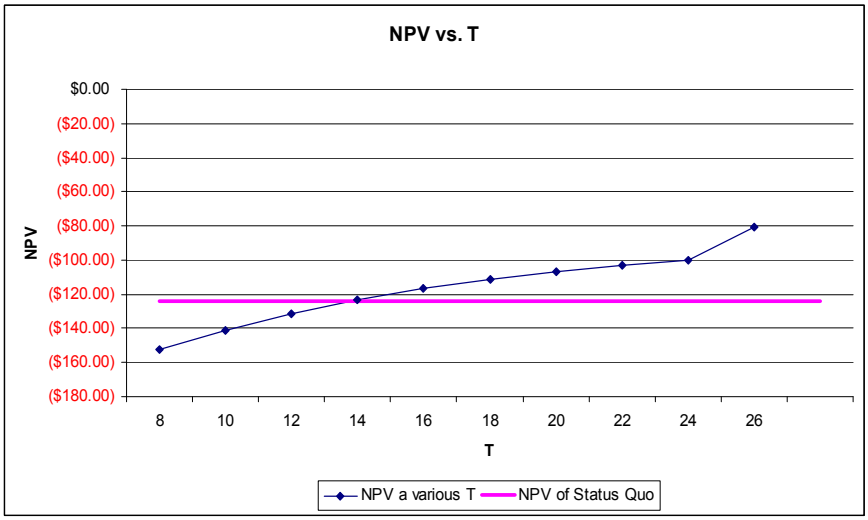
Take note that for this particular example, the remote sensor under consideration is considered to be purely preventive, i.e. its contribution towards reducing the risk is in reducing its likelihood and not in reducing its consequences.

Exhibit 3. Information for Examples 1A and 1B.

	Do-nothing	**Remote Sensor, 1st generation**	**Remote Sensor, 2nd generation**
Initial cost	0	$35M	$35M
Yearly cost	0	$5M	$5M
T	5 years	? years	? years
C	$200M	$200M	$150M
NPV	-$124M	?	?
Discount rate = 10%			

Step 5 – Cost and benefit analysis. Since the effectiveness of the remote sensor to delay the explosion of dirty bomb is not known, the risk manager can then perform sensitivity analysis on what values of T will make this technology worth its cost compared to doing nothing. Exhibit 4 shows that based on the NPV criterion, the remote sensor needs to be effective enough to delay the dirty bomb explosion by at least 14 years (T >= 14) to make it worth its cost. That is, the remote sensor will have better NPV than doing nothing if it can delay the dirty bomb explosion by at least 14 years.

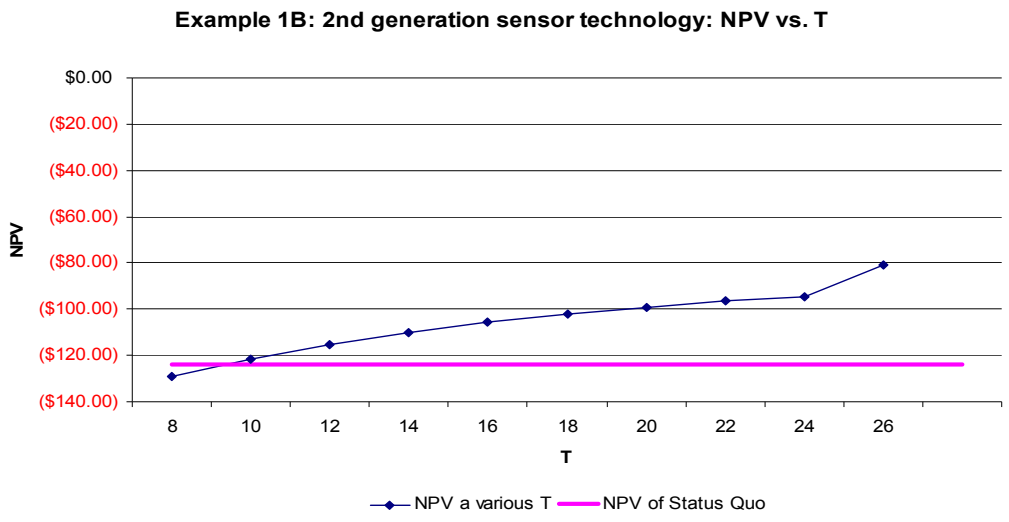
Exhibit 4. NPV for various T for Example 1A.



Step 6 – Resource allocation and iteration. Using the information summarized in Exhibit 4 and all other available information, the decision maker thinks that the current sensor technology will not be able to delay the event by at least 14 years and as such has decided to not do anything. However, new developments in terms of better sensor technology, new intelligence, or policy changes in the near future are almost certain.

Example 1B – 2nd Generation sensor technology with unknown time-to-event T and improved C. Consider the preceding example, but say that since the last analysis, there has been considerable improvement in sensor technology coupled with policies on how information coming from sensors is used in the deployment of emergency management plans. As a result, the sensor technology not only delays the occurrence of the event, but also contributes to decrease the consequence if the event occurs. This new information is represented in the right-most column of Exhibit 3. The analysis using the new sensor technology finds that NPV for implementing the new sensor becomes better than the do-nothing alternative if the new sensor can delay the event by at least 9 years, which now justifies the implementation of the sensor. This is shown in Exhibit 5. This example shows how the Delayed-Bang Approach can be used to re-evaluate security-related decisions consistently even when assumptions change or new information becomes available.

Exhibit 5. NPV for various T for Example 1B.



Example 2 – Stochastic T. The CIO of a data services company wants to evaluate the corporate IT security system. The system consists of eight solutions: Alternatives 1, 2,…, 8. The CIO's objective is to determine which of the Alternatives are economically feasible based on the NPV criterion. To accomplish this evaluation, the CIO assembles a team to model the effectiveness of these solutions. Due to the high degree of uncertainty, the team cannot provide a point estimate for the effectiveness of the Alternatives in terms of T, but rather as a distribution of possible values of T represented by a discrete Uniform distribution.

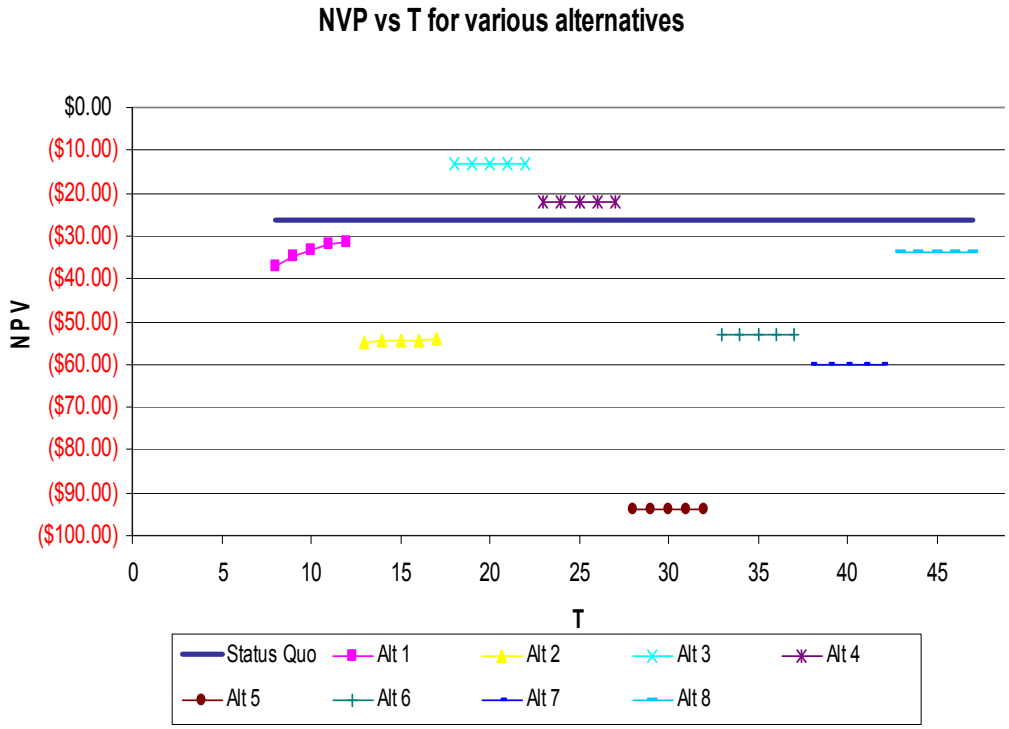
Exhibit 6. Information for Example 2.

Alternative	Initial Cost	Yearly Cost	T = U(a,b,1)
1	20	5	U(8,12,1)
2	40	7	U(13,17,1)
3	35	11	U(18,20,1)
4	10	6	U(23,27,1)
5	50	22	U(28,32,1)
6	25	14	U(32,37,1)
7	28	16	U(38,42,1)
8	18	8	U(43,47,1)
Discount rate = 5%			
Consequence = $200M for all Alternatives			

Similar to the previous example, the status quo or do-nothing alternative is the basis for comparison. The discount rate is 5%. Unlike the previous example where there is unknown T, this example has known Discrete Uniform distribution U (a, b, 1) of T for all 8 alternatives, conceptually similar to Equation 2 discussed earlier for survivability analysis. These are shown in Exhibit 6.

Exhibit 7 shows the NPV for all 8 alternatives as well as the NPV for the do-nothing alternative. The figure shows that Alternatives 3 and 4 are worth their cost while Alternatives 1, 2, 5, 6, 7, 8 are not.

Exhibit 7. NPV for all 8 Alternatives.



Summary

This article presented the Delayed-Bang Approach to the valuation of risk management alternatives in critical infrastructure security. The use of the Delayed-Bang Approach provides a step further than what was possible using the previously developed Risk-Based Return on Investment (RROI) method because of the capability to choose among alternatives for investment rather than simply knowing when to invest more or less.

The significance of the Delayed-Bang Approach is in how three topics, engineering economics, survivability analysis, and probability theory, can be used in a novel way to address sustainability, which currently is an emerging area of security risk management both for public and for-profit organizations. There is also significance in the proposed algorithm as a step towards cost-justifiable resource allocation decisions grounded on a generally acceptable risk management framework by allowing visualization and comprehension of tradeoffs between loss prevention and loss reduction, and the use of temporal information, advances in data fusion, and data mining. It also serves as a foundation for descriptive and prescriptive resource allocation in risk

management, benefit-cost evaluation of risk related resources, and refinement of the concept of the likelihood of a risky event.

References

Arora, A., D. Hall, C. A. Pinto, D. Ramsey, and R. Telang (2004). "Measuring the Risk-Based Value of IT Security Solutions." IEEE IT Professional, v.no.6, pp. 35-42.

Cheng, S., R. Stough, and A. Kocornik-Mina (2006). "Estimating the Economic Consequences of Terrorist Disruptions in the National Capital Region: An Application of Input-Output Analysis." Journal of Homeland Security and Emergency Management: Vol. 3 : Iss. 3, Article 12.

Chisholm, J. (2000). "Benefit-Cost Analysis and Crime Prevention." Australian Institute of Criminology, Trends and Issues in crime and criminal justice, no.147.

Colette, D. (2003). "Modeling Survival Data in Medical Research." Second Ed. Boca Raton: Chapman & Hall/CRC.

Haimes, Y. (1998). "Risk modeling, assessment, and management." J. Wiley & Sons.

Johnson, R.E., and N. Johnson (1980/1999). "Survival Models and Data Analysis", New York: John Wiley & Sons.

Lee, B., P. Gordon, J. Moore II. and H. Richardson (2008). "Simulating the Economic Impacts of a Hypothetical Bio-Terrorist Attack: A Sports Stadium Case." Journal of Homeland Security and Emergency Management: Vol. 5 : Iss. 1, Article 39.

Park, J. Y. (2008). "The Economic Impacts of Dirty Bomb Attacks on the Los Angeles and Long Beach Ports: Applying the Supply-Driven NIEMO (National Interstate Economic Model)." Journal of Homeland Security and Emergency Management: Vol. 5 : Iss. 1, Article 21.

Pinto, C. A., A. Arora, D. Hall, E. Schmitz (March 2006). "Challenges to Sustainable Risk Management: Case Example in Information Network Security." Engineering Management Journal, vol 18(1),

Pinto, C.A. and A. S. Pathak (2008). Title of Abstract: Delayed bang approach: Risk tradeoff between prevention & preparedness. In: Society for Risk Analysis Annual Meeting 2008, Risk Analysis: the Science and the Art; 7-10 November 2008; Boston, MA, USA. Abstract number: W2-J.4.

Rejda, G. E. (2011). "Principles of Risk Management and Insurance", Boston: Prentice Hall.

Rose, A., K. Porter, N. Dash, J. Bouabid, C. Huyck, J. Whitehead, D. Shaw, R. Eguchi, C. Taylor, T. McLane, L. Tobin, P. T. Ganderton, D. Godschalk, A. S. Kiremidjian, K. Tierney, and C. Taylor (November 2007). "West Benefit-Cost Analysis of FEMA Hazard Mitigation Grants." Natural Hazards Rev., Volume 8, Issue 4, pp. 97-111.

Willis, H. H., T. LaTourrette (2008). "Using Probabilistic Terrorism Risk Modeling for Regulatory Benefit-Cost Analysis: Application to the Western Hemisphere Travel Initiative in the Land Environment." Risk Analysis, Vol. 28; Number 2, pp. 325-339.

Yezer, A. M. (2005). "Dealing With Terrorism - Stick or Carrot?" Journal of Homeland Security and Emergency Management: Vol. 2 : Iss. 2, Article 5.