Portfolio Analysis of Layered Security Measures

Samrat Chatterjee[a], Stephen C. Hora[a*], Heather Rosoff[a]

[a]CREATE, University of Southern California

Abstract: Layered defenses are necessary for protecting the public from terrorist attacks. Designing a system of such defensive measures requires consideration of the interaction of these countermeasures. In this article, we present an analysis of a layered security system within the lower Manhattan area. It shows how portfolios of security measures can be evaluated through portfolio decision analysis. Consideration is given to the total benefits and costs of the system. Portfolio diagrams are created that help communicate alternatives among stakeholders who have differing views on the trade-offs between security and economic activity.

Keywords: Portfolio decision analysis, homeland security, terrorism risk, systems analysis, expert elicitation, probabilistic risk assessment

INTRODUCTION

To defend against terrorism, governments adopt a strategy of multiple layers of defense to thwart and respond to attacks of various kinds [1,2]. Some security measures, such as shoe inspection at airports, are effective against a relatively narrow set of attacks while others, such as those entailing wireless surveillance, have a potential for stopping a wide variety of attacks. The Transportation Security Administration (TSA) [3] claims to have twenty layers in its airline security system. Building a layered defense system that is effective in preventing successful attacks and efficient with respect to the consumption of resources is complex and requires one to think about the synergy of various security measures.

In this article, an approach to building a system of layered defenses is discussed in terms of portfolios of security measures. The portfolio approach is proposed as the performance of a system that cannot be inferred from the individual performance of security measures without consideration of how the protective systems work together and how effective they are against various threats[4]. An effective system of security measures work together as a team much as one needs football players to have different capabilities. Moreover, when faced with multiple threats, the layered defense system needs to have sufficiently diverse components such that no gaps are left for adversaries to exploit.

This research was part of the Urban Commerce and Security Study (UCASS)[5] funded by the Science and Technology Directorate of the Department of Homeland Security through its National Centers of Excellence at Rutgers University and the University of Southern California and with the cooperation of the Mineta Transportation Institute at San Jose State University. The study demonstrates how to analyze the trade-offs between security and economic activity in an urban environment. Although the study focused on New York's lower Manhattan Security Area including Wall Street and the World Trade Center, the general methodology is independent of location.

The product of this analysis is an evaluation methodology for various systems of security measures. The analysis separates the benefits and costs in such a way that one can examine alternative layered defenses that vary with both risk and cost. Risk is measured in terms of reduction in expected consequences while costs entail the direct capital and operating costs of security measures as well as the unintended costs they may impose on the economy or, in some cases, collateral benefits.

*Hora@USC.Edu

SECURITY PROBLEM

The problem of terrorism is very complex in that the variations of attacks are great in number as are the types of defenses. To bring the problem to a manageable size, we have selected five scenarios and seven security measures that capture elements common to a larger set of possible scenarios and security measures. For the portfolio analysis, the selected scenarios and security measures provides a concrete set of examples to work from as the modeling methodologies were discussed, developed, and integrated.

Scenarios

A scenario serves to provide a realistic description of the attack under consideration for analysis. Each scenario was developed as a brief narrative describing the attack type, location, and frequency. A concern with reducing the number of scenarios included in the analysis is that it might lead to an underestimation of the total threat likelihood, and thus an undervaluing of the portfolios of security measures as the less the threat, the less the possible risk reduction which is the primary value of security measures. We call this the "completeness" problem and deal with it in much the same way as one scales up from a sample to a population. A total threat is assessed and that total threat probability is then allocated to the reduced set of scenarios so that the sum of the threats from the reduced set of scenarios is the same value as if the entire set of potential scenarios were included.

A set of five scenarios were created, each of which were borrowed from historical and well-known terrorist events. The scenarios were modeled after past major terrorist attacks in Mumbai, India; Tokyo, Japan; Madrid, Spain; London, England; and Israel [5]. Each scenario was accompanied with a brief narrative describing the individual event. The five stylized scenarios are as follows:

> ***S1 (Mumbai):*** *Several small teams of attackers shoot their way into a number of large office buildings and hotels surrounding the World Trade Center construction site and begin a killing rampage.*
>
> ***S2 (Tokyo):*** *In five coordinated attacks, perpetrators release a chemical agent on several lines of the New York City Metro and PATH (The Port Authority of New York and New Jersey) trains passing through Lower Manhattan and the World Train Center Station.*
>
> ***S3 (Madrid):*** *During the peak of New York rush hour, multiple explosions occur aboard New York Metro subway trains heading into Lower Manhattan. These include the 7th Avenue express and local, Lexington Avenue express and local, 8th Avenue express and local, Queens/ Broadway/Brooklyn express and local, and Nassau Street express and local.*
>
> ***S4 (London):*** *Terrorists detonate a large bomb aboard a Manhattan Express bus heading into Lower Manhattan, targeting civilians using New York's public transportation system during the morning rush hour.*
>
> ***S5 (Israel):*** *A terrorist with explosives strapped to his chest detonates a bomb at a checkpoint at an entrance outside of the New York Stock Exchange.*

Security Measures

A security measure, or countermeasure, works to reduce the risk of a threat by deterring the attack, by thwarting an attack, or by reducing the consequences of a successful attack. The effectiveness of a security measure may be different for one type of attack scenario compared to another. Some security measures are designed for a specific attack mode, such as a concealed bomb, while others work more generically against many types of threats. For example, a metal detector (magnetometer) is useful in both deterring and thwarting an attack that employs a metallic weapon such as a gun. Closed circuit

television cameras (CCTVs), on the other hand, can detect suspicious activities of many kinds and have forensic value that may translate into deterrence. Neither of these security measures, however, would reduce the severity of a successful attack as might a stockpile of medical supplies in the case of a biological attack or emergency escape ladders and stairwell lighting in the case of the bombing of a building.

While the number of possible security measures, policies and initiatives are infinite, a set of seven security measures were defined for this study. These security measures were selected because they not only represent a wide range of measures that are available, but also because they are heavily employed within Lower Manhattan (and other urban environments). The selected security measures range from technological to human, visible to invisible, permanent to temporary, and focused on screening people to screening vehicles [5]. The security measure descriptions are as follows:

> ***C1 (Random vehicle inspections)***: *A perimeter of checkpoints at the entry/exits points around Lower Manhattan is established. Security inspections that entail the search of persons and their vehicles are conducted on a random basis.*
>
> ***C2 (Permanent street closures to vehicular traffic)****: A portion of Broad Street in front of the New York Stock Exchange and Federal Hall is closed to vehicular traffic. Pedestrian and bicycle traffic, however, would still be permitted on the sidewalk. Traffic in this area is redirected as appropriate to create minimal disruption for vehicles.*
>
> ***C3 (Temporary perimeters and access control):*** *Street restrictions and security checkpoints affecting pedestrian traffic are put in place. The checkpoints include temporary barricades at various intersections in the area. Anyone traveling into or within the area is subject to a "stop and search" by a uniformed New York police officer.*
>
> ***C4 (Random bag and parcel inspection)****: Security personnel conduct random inspections of bags and parcels at rail and subway stations heading to or leaving Lower Manhattan. The random searches are carried out 24 hours a day, 7 days a week. Police use visual checks, bomb-sniffing dogs, and explosive detection technology to check the bags for hazardous materials.*
>
> ***C5 (X-rays & magnetometers in building lobbies)****: Building security is upgraded by hiring additional protection officers and installing magnetometers to detect metal items, such as guns and knives, and x-ray scanners to inspect bags and packages at the entrances of major/large buildings in Lower Manhattan.*
>
> ***C6 (Increased visible presence of police)****: Police presence is increased throughout Lower Manhattan. Police officers do not target specific individuals, but are instructed to be more vigilant in pursuing tips and leads and analyzing patterns of unusual behavior.*
>
> ***C7 (CCTV cameras)****: An additional 1,700 close-circuit television (CCTV) cameras (resulting in 3,000 cameras total) are located throughout Lower Manhattan. The CCTV cameras help police assess suspicious activity or actual events, reduce incident response time, and create a common technological infrastructure for security surveillance.*

PORTFOLIO MODELING AND ANALYSIS FRAMEWORK

In this section, we describe our modeling and analysis framework and the underlying assumptions. With seven security measures, one can construct $2^7 = 128$ different security portfolios for consideration. Denote the k^{th} security portfolio by set of indicators $\{x_{1k}, x_{2k}, ..., x_{7k}\}$ where $x_{jk} = 1$ if the j^{th} security measure is included in the portfolio and $x_{jk} = 0$ otherwise. The expected annual risk reduction, R_k, and net cost, C_k, are computed as below (see equations 1 and 2). The expected annual

risk reduction formulation is based on fundamental concepts of probability theory [6] where we assume that the security measures operate independently of one another in terms of deterrence and the ability to thwart an attack. Expected annual risk reduction not only depends on the efficacy of the portfolio of security measures but also on the likelihood of an attack and the consequences of a successful attack. The net cost is an aggregation of the direct (capital and operating) and indirect (spillover) costs associated with a security portfolio.

$$R_k = \sum_{i=1}^{M} t_i c_i \left[1 - \prod_{j=1}^{N} (1 - d_{ij} x_{jk})(1 - e_{ij} x_{jk}) \right] \tag{1}$$

$$C_k = \sum_{j=1}^{N} x_{jk} \left(k_j + o_j + s_j \right) \tag{2}$$

where:

t_i is the annual frequency of scenario *i* without the security measures in place;

c_i is the expected consequence of scenario *i* given a successful attack;

d_{ij} is the deterrence effect against scenario *i* of security measure *j*;

e_{ij} is the interdiction effect against scenario *i* of security measure *j*;

k_j is the amortized annual capital cost of security measure *j*;

o_j is the annual operating cost of security measure *j*;

s_j is the indirect benefit/cost or spillover effect of security measure *j* (positive or negative);

M is the number of scenarios; and

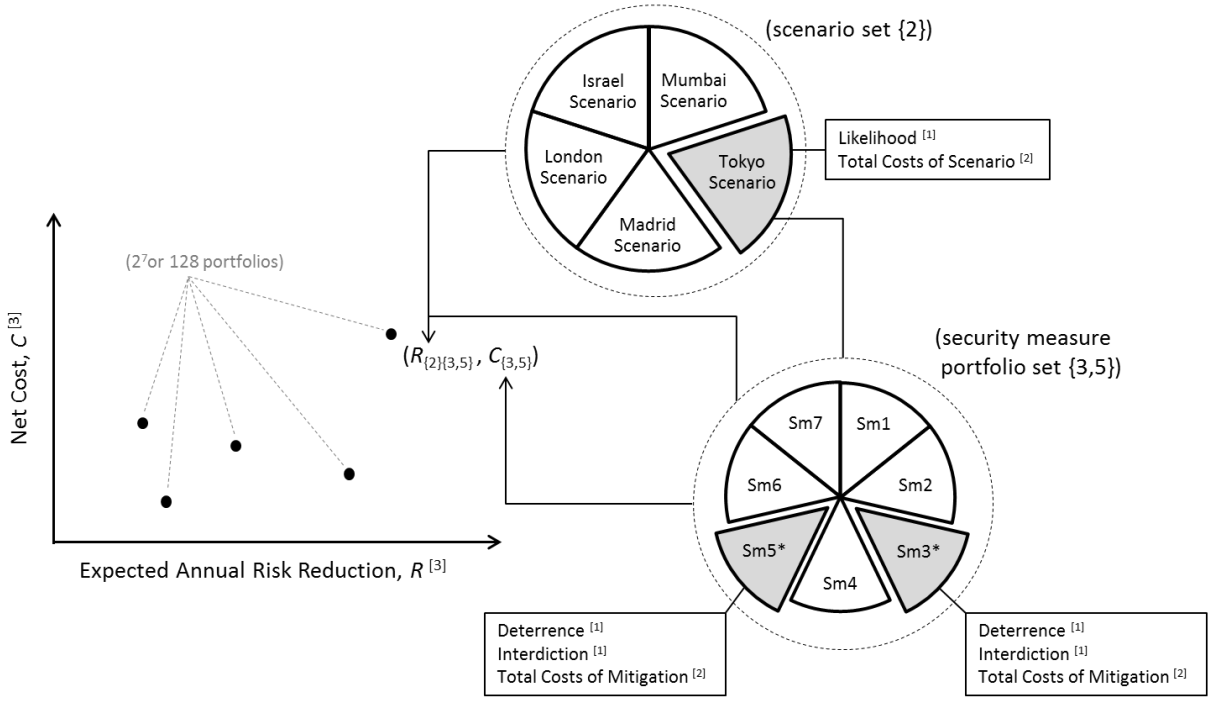
N is the number of security measures.

Equation (1) is developed by considering deterrence and interdiction as distinct benefits of a security measure. Now suppose a threat has an annual frequency *t*, and two security measures are available that reduce the threat through deterrence by a fraction d_1 and d_2 respectively. The frequency of the attack with the first security measure would be $t(1 - d_1)$. Adding the second security measure further reduces the frequency by $(1 - d_2)$ and thus, the threat frequency is $t(1 - d_1)(1 - d_2)$ with both security measures in place. Similarly, the security measures provide reductions in the frequency of successful attacks through interdiction of fractions e_1 and e_2, respectively. The overall frequency of successful attacks with both security measures, following a similar line of reasoning, is $t(1 - d_1)(1- d_2)(1 - e_1)(1 - e_2)$ so that the reduction in the frequency of successful attacks is $t[1 - (1 - d_1)(1- d_2)(1 - e_1)(1 - e_2)]$. Multiplying this last term by the consequence of a successful attack gives the risk reduction for that threat. Finally, summing across all threats gives the total risk reduction as in equation (1).

Figure 1 presents a notional risk reduction versus cost plot and notional pie charts to indicate scenario and portfolio related computation elements in equations (1) and (2). In this figure, we also present the computational approaches we adopted as part of the risk, economic, and portfolio analyses.

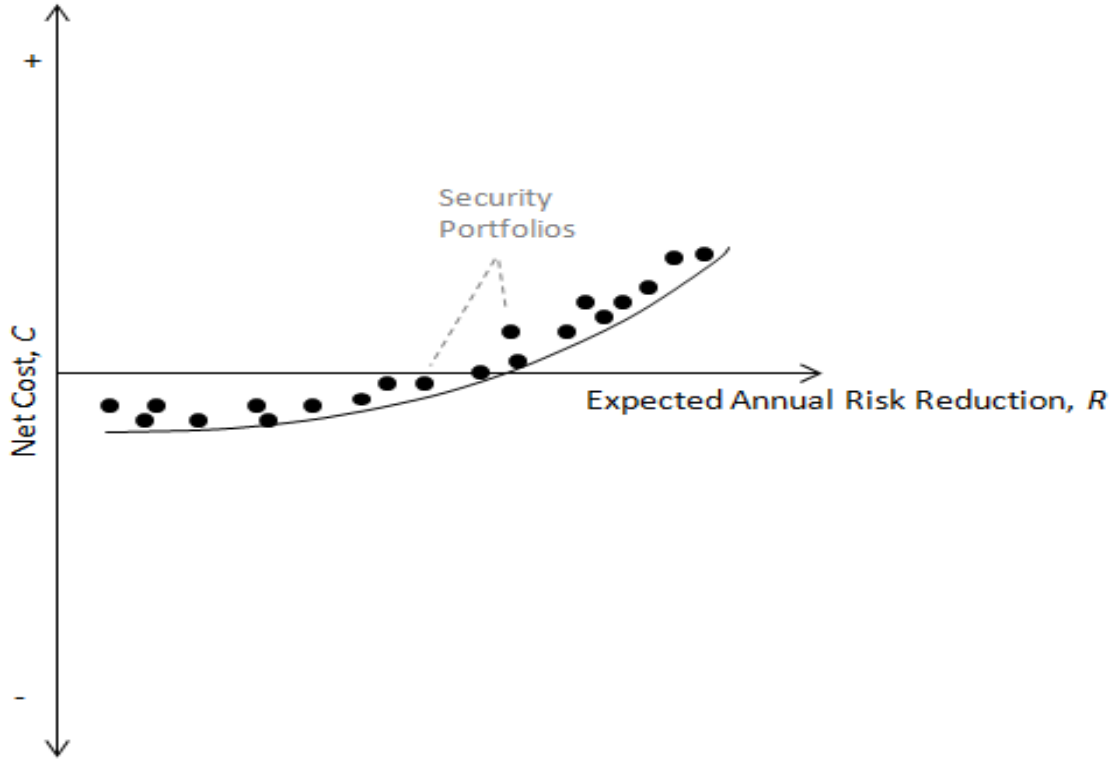
The notional risk reduction versus cost plot in Figure 1 leads to a multi-objective decision making problem of portfolio selection. The decision making objectives include minimizing net cost while maximizing risk reduction. The tradeoff between net cost and corresponding risk reduction may generate an efficient frontier of non-dominated solutions as shown in a notional risk reduction versus cost plot below (see Figure 2). In this figure, for a given level of net cost or risk reduction, the optimal security portfolio falls on the efficient frontier. The efficient frontier consists of those portfolios that cannot be bested simultaneously in both a lower cost and greater annual risk reduction.

Figure 1 Information for Analyzing Security Portfolios



Notes:
[1] Risk Assessment : *Expert Elicitation, Statistical Analysis, Excel VBA Macro*
[2] Economic Analysis : *CGE, Survey, Simulation, Statistical Data Analysis, Literature Synthesis*
[3] Portfolio Analysis : *Excel VBA Macro, Tableau Public Viz*
*Sm3: Temporary perimeters and access control to certain restricted areas of the city
*Sm5: X-rays and magnetometers in building lobbies

Figure 2. Portfolio Analysis Framework



Model Assumptions

Inherent in the portfolio model are assumptions about how the security measures operate, the definition of scenario frequency, and the uncertainties associated with expected annual risk reduction and net costs. More specifically, with regards to security measure operations, it is assumed that they operate independently of one another. This assumption of probabilistic independence is a first order approximation to the interaction of various defensive measures in the portfolio and provides a useful operating assumption unless there are reasons to believe that the measures are redundant or act synergistically. Defensive measures may be redundant if they are different methods of performing the same function. For example, if one has wands to detect metal objects, such as weapons, and has walk through detectors for the same purpose, there is little benefit to adding both measures to the portfolio as long as the capacity of each detector is adequate for the purpose. In this case, one should restrict the set of portfolios considered by excluding redundant security measures.

Sometimes the security measures are partially redundant, so that incremental improvement is obtained. In this case, equation (1) would be modified to include a constructed security measure that represents both security measures in the portfolio and restricts portfolios to contain no more than one of the original two security measures and the constructed security measure. The deterrence and interdiction effects of the constructed security measure would require a separate assessment. The extension to three or more redundant security measures is similar.

Synergistic security measures also may result from one method supporting another. For example, a detection or alarm system provides little interdiction benefit unless forces are available to respond in a timely manner. If the synergism is very high, then a constructed security measure should be used in place of the original security measures, eliminating the indicator variables for both of the original security measures. If synergism is weaker, it may be necessary to employ the same method as when security measures are partially redundant.

The scenario frequencies, t_i, are a parsing of the total estimated annual threat frequency to the set of included scenarios. This is done so that the sum of the likelihoods of the five threat scenarios would be equal to the total threat annual frequency across all possible scenarios whether explicitly included in the analysis or not explicitly included. This allows for a comparison of total security measure costs, which are independent of the specific scenarios, to the estimated total risk reduction. Thus, the five included scenarios are representative of the set of all possible threat scenarios which, while not possible to enumerate, can be assigned a total threat frequency.

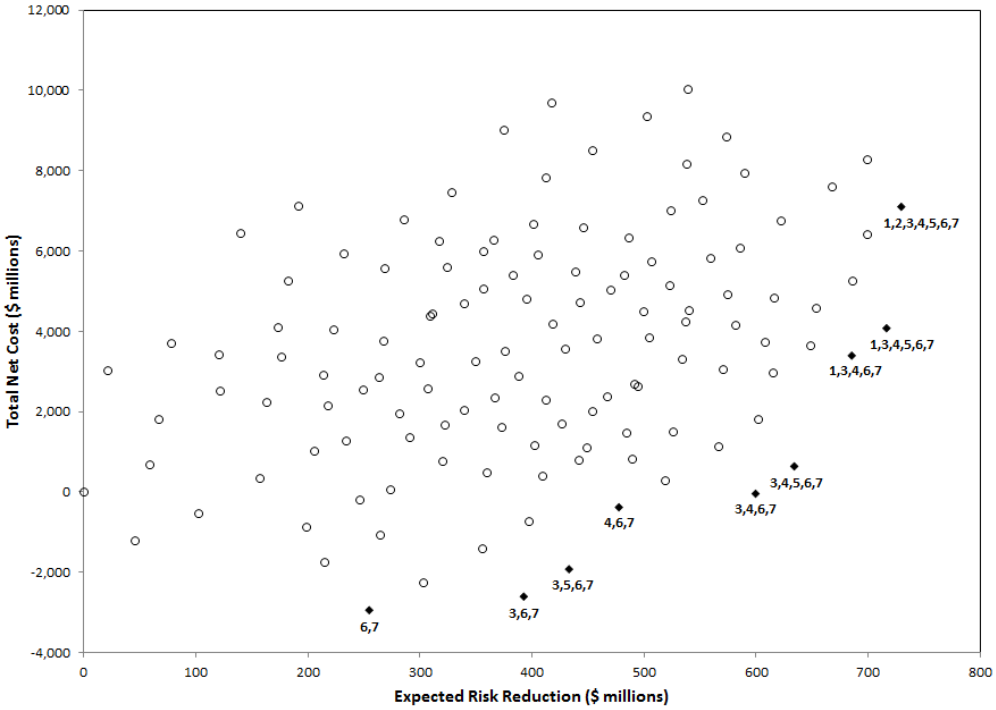
In this analysis, the expected annual risk reduction and net cost in equations (1) and (2) are evaluated as point estimates. In reality, these estimates have uncertainty and may be represented as random variables. A thorough explanation of the direct and indirect cost estimates and the consequence estimates are provided in [7].

RESULTS AND DISCUSSION

Once all possible combinations of security measures have been evaluated in terms of their expected risk reduction and total costs, they can be plotted as points on a portfolio diagram as shown in Figure 5. The benefits/costs that are independent of an attack are shown on the vertical axis and are sensed so that lower costs are preferred to higher costs. When costs are negative, the portfolio has a net benefit independent of any attacks. This occurs for some portfolios because the indirect benefits of having a particular security measure in place outweigh the amortized capital and operating costs. In Figure 3, the horizontal axis shows reduction in expected risk and is positively sensed in that greater reductions are preferred. Risk is the probability of a successful attack times the consequences of that attack.

Given the definition of the axes in the portfolio diagram, a policymaker would prefer portfolios that are found down and to the right in the diagram. Some portfolios will be found to dominate other portfolios in the sense that for the same or lesser cost, the dominating portfolio delivers greater risk reduction. Or, conversely, for the same or higher level of risk reduction the portfolio has lower costs. If one portfolio dominates another it will be found below and to the right of the dominated portfolio, or possibly directly to the right or directly below the dominated portfolio.

Figure 3. Layered Security Portfolios



The portfolios that are not dominated by any other portfolio are members of the efficient set and are those that, all else equal, should be considered as candidates for implementation as they cannot be improved upon simultaneously in both cost and risk reduction. These efficient portfolios are depicted by diamonds rather than disks in Figure 3. Moreover, they are labeled with the security measures included in that particular portfolio.

As the policymaker considers her decision making priorities among the portfolios, she must consider the tradeoff among security and economic activity. Two lines, representing the security and economic activity tradeoff, have been inserted in Figure 4. The upper line passes through all portfolios that have expected risk reduction equal to expected cost. If one is willing to accept that $1 of expected risk reduction is as valuable as $1 in cost reduction, then portfolios above this line have costs that exceed benefits (risk reduction) while those below the line have benefits that exceed costs. The lower line is a translation of the upper line such that all portfolios on the lower line have equal net benefit (risk reduction minus cost) but the net benefits are greater than those of any portfolio on a parallel line above this line. Thus, to identify the optimal portfolio(s) in Figure 4, one should find the parallel line that passes through a portfolio as far down and to the right as possible.

A more risk averse policymaker might consider Figure 5, where the slope of the straight line is increased to 10 implying a willingness to spend $10 up front to avoid $1 in expected loss from an attack. Many would argue that, to date, the $300 billion spent by the Federal Government [8] on preventing terrorism has greatly exceeded this 10:1 ratio. Changing the slope of this line changes the portfolio that has the best risk-reduction and cost profile. The optimal portfolio now shifts up and to the right.

Figure 4. Trade-off 1:1 Cost and Risk Reduction

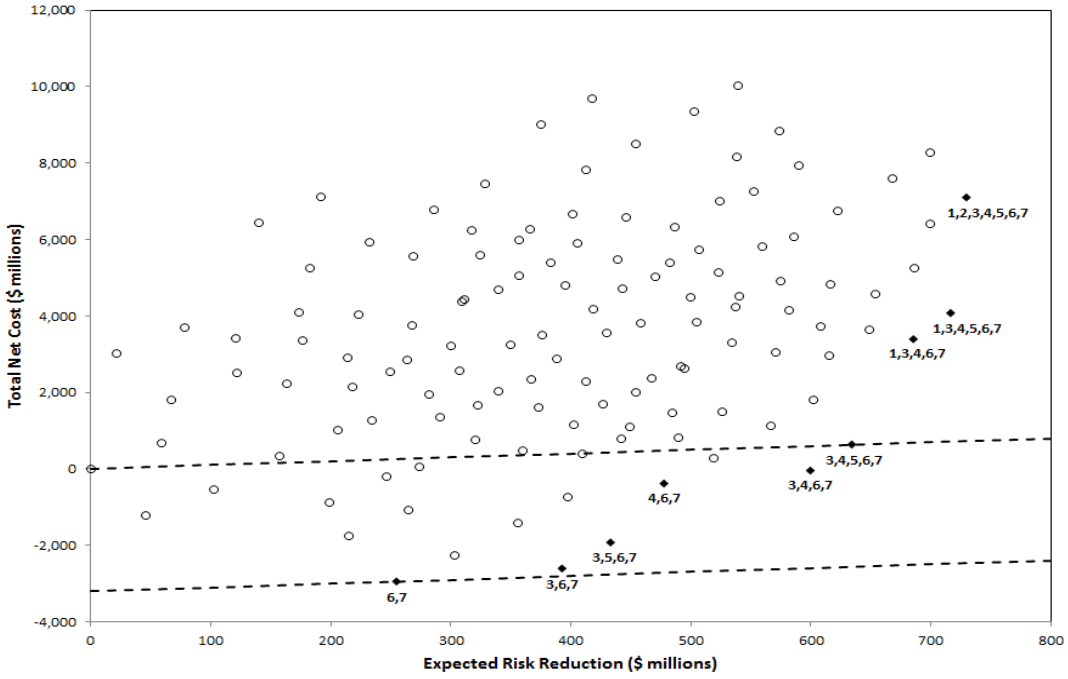
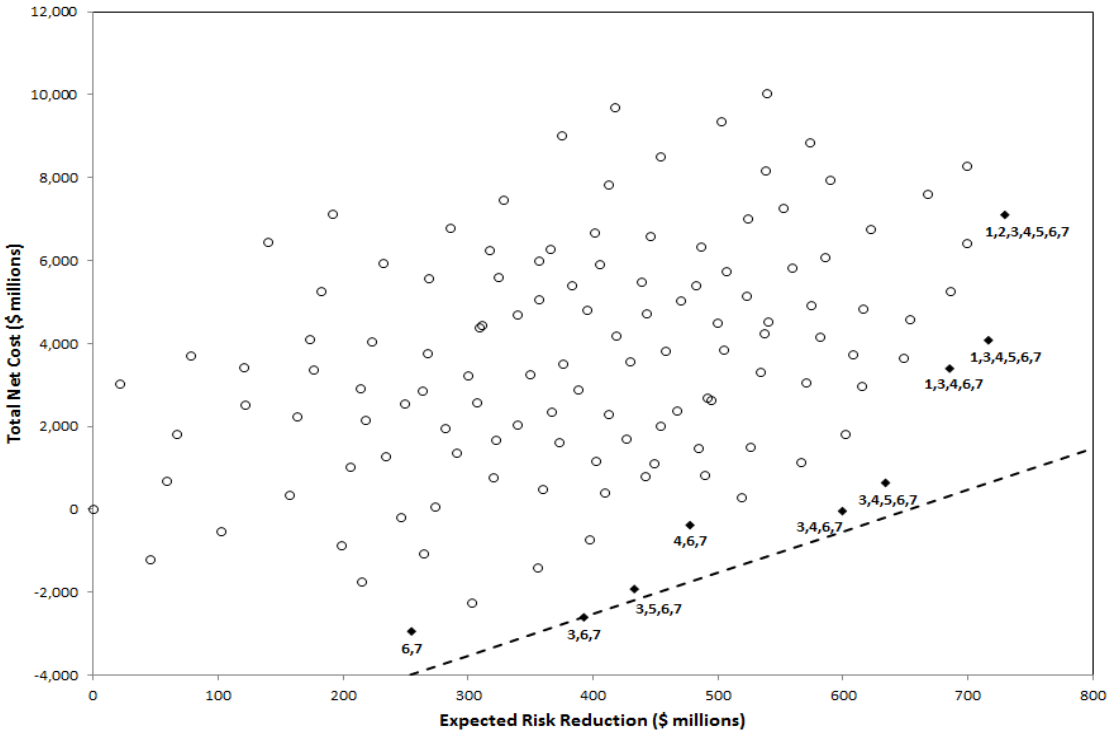


Figure 5. Trade-off 10:1 Cost and Risk Reduction



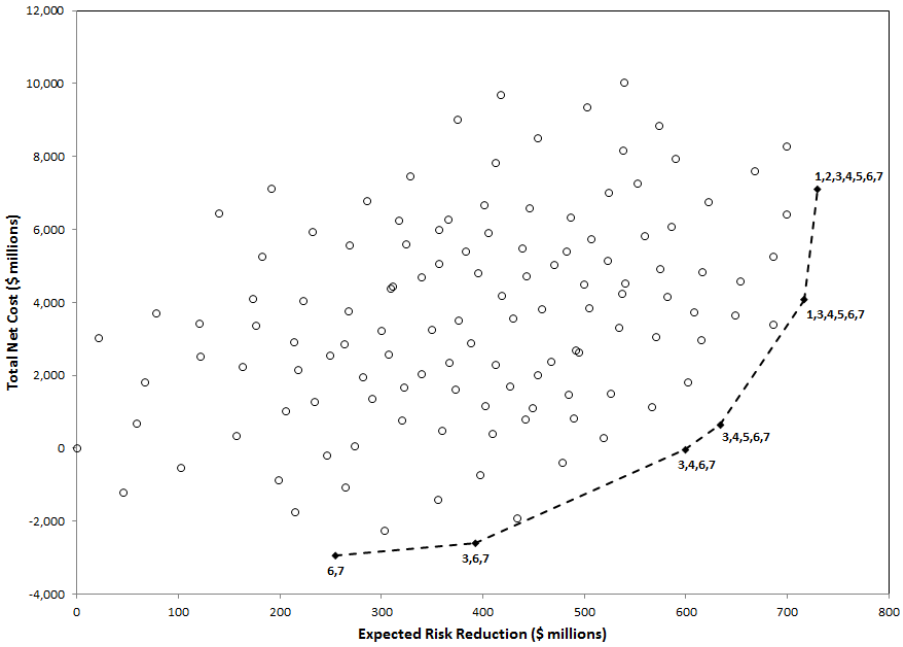
The portfolio diagram cannot answer the question of which portfolio is best, however, unless one is willing to state the appropriate trade-off between pre-event costs and post-event expected losses. Views on these trade-offs will differ among stakeholders. Law enforcement tends to be conservative and invests heavily in prevention; part of a "not on my watch" attitude. Others, such as real estate investors or tour companies, may put greater emphasis on reducing the dampening effects of non-

passive security measures, such as check points or bag inspections. Their trade-off lines would be less steep than those of their law enforcement counterparts.

One might infer that the U.S. Government views the trade-off line to be rather steep as expenditures on preventing terrorist attacks appear to be high relative to the expected risk reduction. This may be due in part to how a human life is valued. Here, the U.S. Department of Transportation value $6.2 million dollars for the loss of a life [9] has been used. It may be that in allocating funding to counter terrorism activities, the Government implicitly uses a higher figure for the loss of life due to terrorism vs. loss of life due to traffic accidents or other more common causes. See the work by Viscusi [10]for interesting evidence related to this issue.

The set of portfolios that should be considered can be reduced further if one assumes that the trade-off ratio between pre-event costs and risk reduction is constant and thus the trade-off line is linear. Those portfolios that form a convex hull are those that are candidates to be on such a linear segment. This assumption results in the exclusion of some portfolios that, although not dominated by any single portfolio, are dominated by a positive linear combination two other portfolios. This is demonstrated in Figure 6 where there are just 6 portfolios that should be under consideration given the linearity assumption.

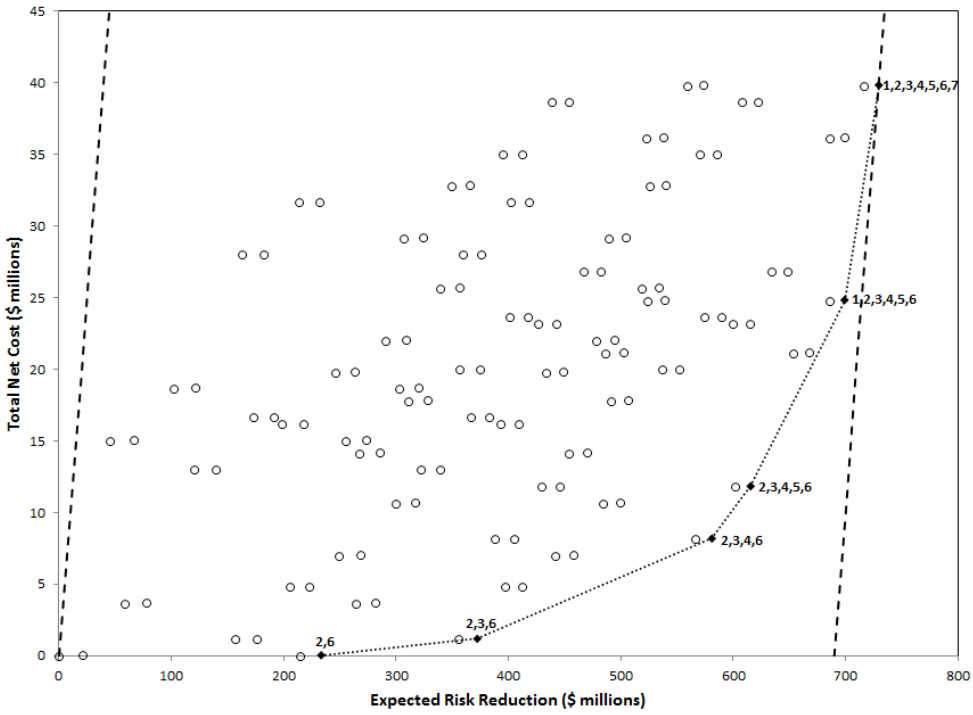
Figure 6. Best Portfolios under Linear Trade-offs



Lastly, as seen in Figure 6, benefits and costs may accrue disproportionately for various stakeholders. For example, law enforcement agencies may be responsible for purchasing and operating CCTVs. For this reason, they may not wish to consider the benefits of CCTVs as the law enforcement mandate is security and not economic development. Law enforcement may consider it inappropriate to use their budget for any purpose other than security and, therefore, may choose to ignore any benefits that are not the direct result of risk reduction. Similarly, the indirect economic burdens brought on by delays, congestion, and inconvenience may not be taken into account because they are not borne by those choosing the security measures. Figure 9 shows the portfolio diagram with spillover costs and benefits removed. This might be the diagram that law enforcement would choose to use in selecting a portfolio rather than the diagram in Figure 6. Note that the scales on the vertical axes in Figures 4 and 7 are very different. The dark lines slightly slanted from vertical in Figure 7 are, in fact, the one-to-

one tradeoff lines for risk reduction and cost and serve the same purpose as the similar lines in Figure 4.

Figure 7. Portfolios without Spillover Effects



One observation derived from the comparison of Figures 4 and 7 is that the entry of CCTV cameras into efficient portfolios is delayed when spillover effects are ignored. This is not surprising, as one might expect, since CCTV systems provide security without active interference and, thus, may enhance perceived wellbeing and economic activity. A more global observation is that with one-to-one trade-offs between costs and risk reduction, ignoring spillover effects makes all portfolios have greater benefits than costs and the best of these becomes the portfolio with all security measures included.

CONCLUSIONS

Decisions about security measures are often made in isolation, considering one measure at a time. A better approach, however, is to consider the security measures together as a system of systems that can be optimized only by considering the interactions among the component systems. The capabilities of the component systems may vary with the type of attack as will the interactions among the capabilities. A portfolio of component systems should be selected to minimize "holes" or weak points which will simply attract attacks.

The benefits and costs of a security system will accrue to different parties unequally. By considering spillover effects, both positive and negative, one attains a more accurate picture of the total benefits and costs to our nation. Myopic decision making where total benefits and costs are ignored can lead to suboptimization. In the example presented here for the Lower Manhattan security area, exclusion of spillover effects can result in significant overinvestment in security and a loss of societal net benefits because too much security can have a dampening effect on economic and social activities.

The portfolio approach to layered security does not prescribe a single solution, but instead provides a number of potential solutions while excluding some configurations that have been identified as dominated. This analysis is not only useful as a pruning device to focus attention on a smaller set of

candidate portfolios, but it also provides a basis for communication and negotiation among stakeholder groups who have differing views on the benefits and burdens of enhanced security.

ACKNOWLEGEMENT

This research was supported by the United States Department of Homeland Security through the National Center for Risk and Economic Analysis of Terrorism Events (CREATE) under Cooperative Agreement No. 2010-ST-061-RE0001. However, any opinions, findings, and conclusions or recommendations in this document are those of the authors and do not necessarily reflect views of the United States Department of Homeland Security or the University of Southern California.

REFERENCES

[1] Lehrman TD. Building a Layered Defense to Combat Weapons of Mass Destruction. Remarks to the NPT Conference, Washington College of Law, American University, Washington, D.C., February 9, 2006.
[2] Department of Defense. Strategy for Homeland Defense and Civil Support, Washington D.C., 2005.
[3] Transportation Security Administration. Layers of Security, 2013. Available at: http://www.tsa.gov/about-tsa/layers-security, Accessed on September 5, 2013.
[4] Buede DM. The Engineering Design of Systems: Models and Methods. New York: John Wiley & Sons, 2011.
[5] Roberts F, Hora S, Jenkins B. Urban Commerce and Security Study Technical Report. Division of Science and Technology, Department of Homeland Security, Washington D.C., June 2013.
[6] Ross S. A First Course in Probability. Delhi, India: Pearson Education, 6th Edition, 2004.
[7] Rose, A., M. Avetisyan and S. Chatterjee. A Framework for Analyzing the Economic Tradeoffs between Urban Commerce and Security, forthcoming in Risk Analysis.
[8]Stewart MG. Risk-Informed Decision Support for Assessing the Costs and Benefits of Counter-terrorism Protective Measures for Infrastructure. International Journal of Critical Infrastructure Protection, 2010; 3: 29-40.
[9] Trottenberg P, Rivkin R. Memorandum to Secretarial Offices and Modal Administrators: Treatment of the Economic Value of a Statistical Life in Departmental Analysis- 2011 Interim Adjustment, U.S. Department of Transportation, 2011. Available at: http://www.dot.gov/sites/dot.dev/files/docs/Value_of_Life_Guidance_2011_Update_07-29-2011.pdf, Accessed on September 5, 2013.
[10] Viscusi WK. Valuing Risks of Death from Terrorism and Natural Disasters. Journal of Risk and Uncertainty, 2009; 38: 191-213.