TECHNICAL ARTICLE

Risk Mitigation Plan for Optimizing Protection of Constructed Facilities

Dr. Harold E. Marshall, Robert E. Chapman, and Chi J. Leng

ABSTRACT: Owners and managers of constructed facilities need help in optimizing protection against natural hazards and terrorist acts that occur infrequently, but result in devastating damages. The World Trade Center and Pentagon attacks in 2001 magnified this need in the minds of facility designers, constructors, owners, insurers, and occupants. This article describes a three-step protocol for satisfying this need. Step 1 is to assess the risk of uncertain, costly, man-made and natural hazards, including terrorism, floods, earthquakes, and fire. A summary of constructed facilities in the US, by type, number, and measures of area, establishes the potential for damages. Described tools for evaluating risk are the Construction Industry Institute Security Rating Index and the RAMPART software product. Step 2 is to identify alternative risk mitigation strategies, used singly or in combination, to reduce the expected value of damages from such events. Potential strategies include engineering alternatives, management practices, and financial mechanisms. Step 3 is to evaluate the life-cycle economic effectiveness of alternative mitigation strategies. Economic methods based on the American Society for Testing and Materials (ASTM) standard practices and software for implementing the methods are described. A case study for a typical commercial building shows how to measure outcomes from alternative terrorist mitigation measures and choose the optimal protection package based on life-cycle cost analysis. Single value estimates and sensitivity analysis descriptions of the economic measures support a combination of renovation investments to protect the building.

KEY WORDS: Disasters, economics, life-cycle costing, optimization, risk mitigation, terrorism

Designers, owners, managers, and occupants of constructed facilities in the US are making dramatic changes to the way they think about their facilities as a result of the 11 September 2001 terrorist attacks on the Pentagon and the World Trade Center. The estimated 19 billion dollars of insured property losses from that day's events was over 20 times the insured loss of the next most costly terrorist event in the world, a bomb in London in 1993, and over 150 times the insured loss of the Oklahoma City bombing in the US in 1995. Moreover, there were 3,132 lives that were lost as a result of the four 9/11 plane crashes [5].

The magnitude of these losses is forcing public and private owners and managers to consider the potential terrorist threats against the facilities for which they are responsible and to plan for ways to avoid and mitigate any damages resulting from terrorist actions. Emerging from this new focus on planning for protection against terrorism is the realization that it makes sense to evaluate all kinds of disasters, man-made and natural, as a group. Costs for protection against multiple hazards can be shared among the hazards protected against, thereby reducing the cost for any single form of protection. Or, looked at another way, a given cost of protection can yield extra benefits when considering multiple hazards. For example, a strengthened or hardened structural bridge design provides protection against both an earthquake and a terrorist explosive charge. This spillover of benefits from one kind of protection to another has highlighted the need for a holistic approach to planning protection against multiple hazards.

Purpose and Scope

This article presents a three-step protocol for developing a risk-mitigation plan for optimizing protection of constructed facilities. This protocol helps users determine the vulnerability of their facility to damages from multiple, uncertain, disastrous events; identify engineering, management, and financial strategies for abating the risk of damages; and use economic evaluation to select the optimum package of risk mitigation strategies to protect their facility.

A classification of hazard types, such as chemical or explosive, identifies potential problem events. A classification of sources of potential hazards, natural and man-made, informs facility managers as to the possible origins of potential hazards. A summary of constructed facilities, with statistics on number of units and measures of area, provides perspective on the critical infrastructure at risk in the US.

Explanations of selected risk assessment tools help prospective users assess risks facing their facility. Examples of engineering, management, and financial strategies help readers identify approaches for abating the risk of damages to their facilities. Descriptions of economic methods and an economic evaluation case study provide measures of economic merit and an illustration of their use in arriving at the optimal package of risk mitigation strategies.

The ultimate purpose is to help users select the combination of disaster mitigation strategies that minimize the sum of costs of protection and expected value of damages. The three-step protocol applies both to facilities in use, as well as those on the drawing board.

Types and Consequences of Hazards to Constructed Facilities

Constructed facilities are at risk of damage from both natural and man-made hazards. Mitigation of natural hazards is based on improving protection and reducing damage. Mitigation of man-made hazards is based on a greater range of approaches: prevention, detection, deterrence, and protection.

Natural Hazards

The risk of natural hazards varies across geographic areas and from season to season. Figure 1 provides data for the US on residential and commercial property losses resulting from flooding, high winds, earthquakes, wildfires, and other natural hazards from 1996 to 2002.

Man-made Hazards

Like natural hazards, the risks of man-made hazards may also vary from city to city and year to year. Assessment of some type of these risks is complicated by the infrequency of event. Man-made hazards to constructed facilities include chemical, biological, radiological, explosive (CBRE), or other threats. These hazards are realized through industrial accidents, arson and accidental fires, sabotage, workplace violence, civil unrest, conventional war, and terrorism. Man-made hazards vary by intent (industrial accidents versus sabotage, for example) and by scale. Small-scale terrorism may involve a lone gunman, for example, in contrast to larger-scale terrorist attacks intended to inflict massive casualties, property destruction, and psychological trauma among a larger, more geographically dispersed population.

Between 1975 and 2003, there have been at least 28 significant CBRE man-made incidents or attempts affecting US constructed facilities domestically or overseas, according to the US Department of State [16]. Of these incidents, one was a radiological threat (1979 nuclear reactor accident at Three Mile Island), one was a biological attack (2001 anthrax contamination spread through the US Postal Service), one was a chemical threat (1983 leak at the Union Carbide pesticide plant in Bhopal, India), and 25 involved explosives. The explosive-type incidents ranged in scale from letter bombs, to the rocket-propelled grenade

fired through a window of the US Embassy in Moscow in 1995, to the 9.1 metric ton to 13.6 metric ton (10 short ton to 15 short ton) fuel truck bomb that exploded outside the Khobal Towers in Saudi Arabia in 1996, to the hijacked airliners crashing into the World Trade Center towers and Pentagon in 2001.

Table 1 details insured losses and costs attributed to selected terrorist incidents in the US over the last decade. The explosive attacks on the World Trade Center and the Murrah Federal Building, the crash of the hijacked airliners into the Twin Towers, and the anthrax attacks highlight the need to address these hazards in spite of their relative infrequency.

Fire hazards, other than wildfires, have imposed high costs to US constructed facilities. This hazard exhibits varying levels of intent, from arson to negligence to accidents. In most years, the damage and costs of these fires far exceed those resulting from other man-made hazards. For non-residential buildings, for example, these fires damaged nearly 150,000 structures and caused losses of nearly $2.9 billion, on average, each year during 1989-2001 (excluding September 11th losses). Fire damage of residential structures is even greater: in an average year during the same period, 435,000 structures suffered fire losses totaling $4.7 billion [8].

Industrial accidents also pose risks to constructed facilities and their occupants. Unlike many of the man-made hazards, industrial accidents are not purposive. Mitigation can limit their negative consequences, and preemptive measures and safeguards can prevent or reduce the likelihood of occurrences. Like arson, the frequency of industrial accidents may be greater than that of sabotage, workplace violence, civil unrest, conventional war, and terrorism. For example, between August 4-8, 2003, there were 15 chemical accidents in the US reported to the US Chemical Safety and Hazard Investigation Board Chemical Incident Reports Center. Fatalities were reported at three of the accidents [12]. The relative frequencies and consequences of these natural and man-made hazards to constructed facilities are critical to the determination of appropriate measures to mitigate risks.

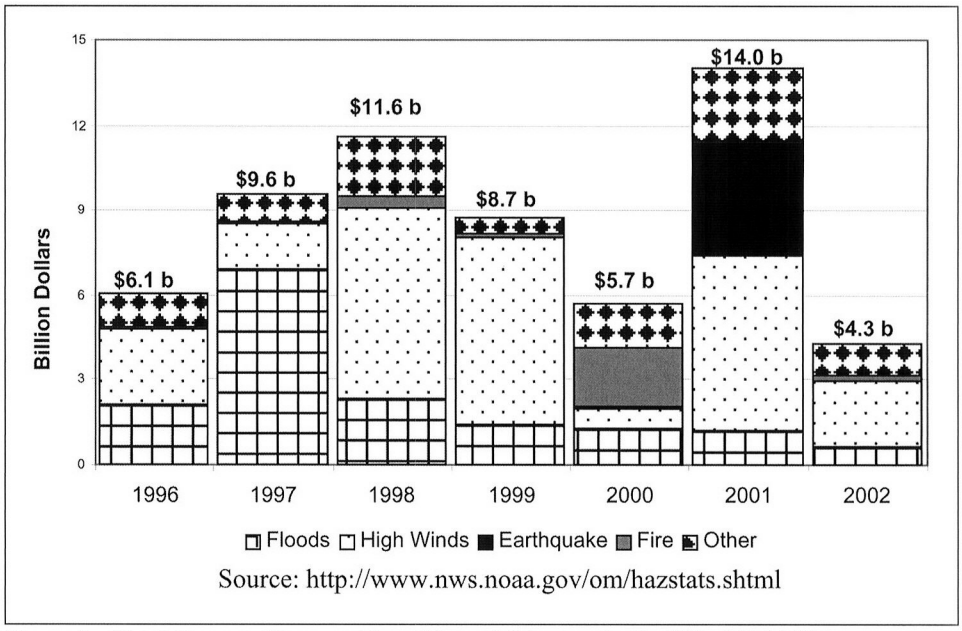

Figure 1—Total Property Damage From Natural Disasters in the US - 1996-2002

Constructed Facilities at Risk

Constructed facilities include infrastructure, non-residential buildings, and industrial facilities. Infrastructure includes transportation, water resource management, and energy delivery facilities. Examples of nonresidential buildings are offices, education, health care, and mercantile buildings. Industrial facilities include oil refining, chemical manufacturing, and power plants. Although this article focuses on the protection decisions facing owners and managers of constructed facilities, the protocol developed in this article also applies to residential buildings.

Typical measures of the value of constructed facilities are replacement cost, their content's value, or the value of the services and use that they provide. Other facilities have historic or symbolic value; loss or damage to these facilities may impose substantial cultural, psychic, or emotional costs on the populace.

Table 2 describes a selected stock of critical assets in the US. Assets include energy production and generation, the nation's telecommunications infrastructure, and passenger and freight transportation networks. These assets provide services critical to the smooth functioning of the US economy.

Incident	Fatalities & Injuries	Insured Losses/Cost
Bomb explosion in World Trade Center garage February 26, 1993, New York City	6 fatalities; 1,000 injured	$725 million
Truck bombing of Alfred P. Murrah Federal Building April 19, 1995, Oklahoma City	166 fatalities; 467 injured	$145 million
Airline attacks at Pentagon, World Trade Center, and southern Pennsylvania September 11, 2001, Washington, D.C., New York City, and Shanksville, Pennsylvania	3,132 fatalities; 2,250 injured	$40.2 billion†
Anthrax assault through U.S. Postal Service October 2001, various locations	5 fatalities; 13 other confirmed infections	$929 million‡
Sources: SwissRe, "Terrorism--Dealing with a New Spectre," Focus Report (2002); U.S. Postal Service, 2001 Comprehensive Statement on Postal Operations. (United States Postal Service: 2001). Available at: http://www.usps.com/history/cs01/cs2001.pdf; Hartwig, Robert, "The Long Shadow of September 11: Terrorism and Its Impacts on Insurance and Reinsurance Markets." † Includes business interruption and aviation hull losses. ‡ Estimated Fiscal Year 2002 costs to U.S. Postal Service of operations disruptions and expenditures to remediate anthrax contamination, including medical treatment, protective equipment, testing and clean-up, education, detection equipment, and security initiatives.		

Table 1—Insured Losses From Selected Man-Made Incidents in the US

Asset Type	Number	Units
Electricity	2,800	Power plants
	130 million	Households and institutions served
	12.96 trillion (3.6 trillion)	MJ (KWh) consumed (2001)
Nuclear Power Plants	104	Commercial plants
	20 %	U.S. electrical generation capacity
Oil and Natural Gas	300,000	Producing sites
	4,000	Off-shore platforms
	Over 600	Natural gas processing plants
	153	Refineries
	Over 1,400	Product terminals
	7,500	Bulk stations
Chemical Industry & Hazardous Materials	66,000	Plants
Telecommunications	3.2 (2.0) billion	Kilometers (Miles) of cable
	20,000	Physical facilities
Aviation	5,000	Public airports
Railroads	193,080 (120,000)	Kilometers (Miles) of major railroads
	20 million	Inner city resident use annually
	45 million	Passengers on trains and subways
Highway Bridges	590,000	Highway bridges
Pipelines	3.2 (2.0) million	Kilometers (Miles) of pipelines
Maritime	300	Inland or coastal ports
Mass transit	500	Major urban public transit operators
Dams	80,000	Dams
Source: *The National Strategy for the Physical Protection of Critical Infrastructures and Key Assets*, Executive Office of the President, February 2003.		

Table 2—Critical Assets in the US:2003

Disruptions in the service of these assets can quickly ripple throughout the nation, as occurred during the August 14-15, 2003 power grid failure in sections of the northeastern US and southeastern Canada.

The value of commercial real estate in the US is an estimated $10.6 trillion. Of this amount, $5.5 trillion, or 52 percent, represents the replacement cost of structures, $3.7 trillion (35 percent) represents equipment and software, and $1.4 trillion (13 percent) represents inventory [5]. Table 3 shows that nonresidential buildings and industrial buildings in the US in 1998-1999, numbered almost 4.9 million, encompassing nearly 7.5 billion square meters (m^2) (over 80 billion square feet (ft^2)). Clearly the owners of constructed facilities cannot afford to invest in protective measures for all of these structures.

Risk Mitigation Plan

A three-step protocol for developing a risk-mitigation plan for optimizing protection of constructed facilities is proposed. Step 1 is to assess the risk of uncertain, costly, man-made and natural hazards, including terrorism, floods, earthquakes, and fire. Because resources are too limited to allow for full protection of all facilities against every possible hazard, economic efficiency dictates that investments for protection be a function of the likelihood of a disaster occurring, the expected value of damages, and the cost of protection. By assessing the risk facing a facility and the likely damages that might result from various disasters, decision makers can determine if a facility merits some degree of protection. The next section of this article, "*Risk Assessment Tools*," describes software and other tools for assessing facility risk.

The second step in the plan is to identify engineering, management, and financial strategies to abate the risk of damages. To protect a property, facility decision makers tend to think first of physical barriers or heightened security regarding access. Yet there are numerous alternatives for protection against losses, such as insurance, that are often overlooked. Some strategies will lower the probability of the disaster occurring, while others will lower the damages incurred once the disaster happens. This article's section on "*Mitigation Strategies*" describes different types of strategies and how they affect the economic bottom line of the facility stakeholder.

The third step is to use economic analysis to select the optimum package of risk mitigation strategies. More attention is devoted to this step than to the other two because economic analysis determines final protection strategy choices. This article's section on "*Economic Evaluation*" describes ASTM standard measures of economic merit for evaluating alternative mitigation strategies.

Risk Assessment Tools

Several organizations have developed risk assessment tools to model terrorist behavior, as well as risks from natural hazards and other man-made hazards. Some tools are software based, which enables users to generate customized assessments. Others are publications, which provide more general guidance about vulnerabilities and remediation methods.

Software-Based Assessment Tools

One software-based risk assessment tool is the Risk Assessment Method—Property Analysis and Ranking Tool (RAMPART)[7], sponsored by the General Services Administration (GSA) and developed at Sandia National Laboratories. RAMPART combines building and site-specific information with geographic seismic, weather, and crime data, using its expert system of rules to predict the vulnerability of a building to consequences resulting from natural hazards (hurricanes, earthquakes, flooding, and winter storms) and man-made hazards (crime inside the building, crime outside the building, and terrorism).

Another software product that can be used to assess the vulnerability of constructed facilities is the US National Institute of Standards and Technology's (NIST) CONTAMW [4]. CONTAMW captures user-defined building structure characteristics to

Building Characteristics	Office	Education	Health Care	Mercantile /Service	Industrial	Other	All
Number of Buildings (thousands)	739	327	127	1,145	227	2,319	4,884
Building Floorspace (million m^2)	1,119	804	271	1,281	1,193	2,781	7,449
Building Floorspace (million ft^2)	12,044	8,651	2,918	13,786	12,836	29,939	80,174
Average Building Floorspace (m^2)	1,514	2,459	2,134	1,119	5,256	1,199	1,525
Average Building Floorspace (ft^2)	16,298	26,456	22,976	12,040	56,546	12,910	16,416
Sources: U.S. Department of Energy's CBECS (1999). Industrial building data from U.S. Department of Energy's MECS (1998).							

Table 3— Buildings at Risk: 1998, 1999

simulate and model the spatial distribution of airborne contamination over time, based on information about the physical properties of the contaminants and design characteristics of the structure and its subsystems. This analysis tool could be used for the probabilistic assessment of damage under chemical or biological attack scenarios. It was used to model the transport of the anthrax spores in the Hart Senate Office Building in October 2001, to evaluate how best to manage the heating, ventilating, and air conditioning (HVAC) system and building space to minimize spread of the disease. It provides important input data for evaluation of risk mitigation measures relating to emergency first responders and building egress.

Risk Assessment Guidance

In addition to these software products, several guidance documents are available to provide facility managers with some direction in assessing the risks facing their structures. Two FEMA publications, *Understanding Your Risks: Identifying Hazards and Estimating Losses* [15] and *Integrating Human-Caused Hazards Into Mitigation Planning* [14], address the need for risk assessment for a variety of hazards. The US Department of Defense (DOD) has approved for public release the *Uniform Facilities Criteria* (UFC), *DOD Minimum Antiterrorism Standards for Buildings*, which was developed with the objective of minimizing the likelihood of mass casualties among DOD personnel from terrorist attacks [13]. Although the UFC system applies to the military departments, DOD agencies, and DOD field activities, the standards identify and highlight several key aspects of site planning, structural design, architectural design, and electrical and mechanical design that play a role in protecting buildings from explosives.

Several industry and professional associations have also developed risk assessment guidance documents. The Construction Industry Institute (CII) is conducting a study sponsored by NIST to identify best practices related to the security of capital facilities projects for critical industries. The findings of the CII-NIST study will provide the basis for assessing the impacts of these practices on cost, schedule, and safety. The study will produce a project security handbook and a security-rating index (SRI). The SRI is a measure of the level of implementation of security practices during the planning and delivery of a project and will quantify assessments of the process of incorporating security into projects.

The American Management Association (AMA) has recently published **The Facility Manager's Emergency Preparedness Handbook** [9]. This handbook is intended to serve as a reference for emergency preparedness planning. It provides guidelines, tools, and checklists to facility managers to prepare for several types of emergencies, such as lockout, terrorism, and workplace violence.

In 2003, R.S. Means published **Building Security: Strategies & Costs** [11], which was intended to assist building and facility owners and managers to assess risk and vulnerability to their buildings, develop emergency response plans, and make choices about protective measures and designs. It provides descriptions and cost information about several types of protective elements and materials.

Mitigation Strategies

Mitigation strategies reduce expected damages from a hazard. A strategy may be aimed at preventing the hazardous event, such as apprehending a terrorist before a bomb can be detonated. A strategy might also be designed to prevent or limit property damages and injuries from a realized hazardous event. An example would be investing in barriers to keep water away from property before flooding occurs. Finally, strategies can be used as policy instruments to encourage or discourage behaviors or investments to make facilities safer. US federal cost sharing on large water projects, for example, encourages local communities to construct facilities for flood control.

Mitigation strategies can be used singly or in combination to protect against a given hazard. A barrier to unauthorized entry might be used in combination with surveillance cameras and a high efficiency HVAC system, for example, to protect against anthrax contamination of a building.

Single strategies can be used to protect against one or more disaster threats. For example, a facility hardened to be bomb and impact resistant would also likely be resistant to high winds and earthquakes.

A single strategy might generate benefits or spillovers aside from disaster mitigation objectives. An improved security system for protection against terrorists, for example, also protects the organization from theft. An improved egress system for evacuation during a terrorist event would also yield spillover benefits from fewer injuries resulting from a non-terrorist-related fire. And filters in an HVAC system that can scrub biological and chemical contaminants will likely raise the quality of air in a facility and thereby increase productivity through reduced lost workdays from sickness.

Most mitigation strategies can be classified as one of the following three types: engineering, management, and financial. The following three sections of this article describe these in detail.

Engineering Alternatives

Engineering alternatives for increased facility protection include structural/material changes, barriers, and mechanical system changes. Dams, levees, and chanelization are structural approaches to protecting facilities from flooding. Constructing stronger and larger bridge piers makes bridges more resistant to damages both from earthquakes and terrorist attacks. Walls, fences, boulders, and large planters are some of the many types of structural barriers that are being used to protect facilities against terrorist attacks. Bullet-proof glass is a material option for greater security.

Other changes include alterations to the HVAC systems; people-moving systems; security system of alarms, sensors/detectors, and facility access screening equipment; and cyber security hardware and software. HVAC systems with high-technology sensors, sophisticated air controls, and efficient filters can "sniff" out

terrorist-delivered chemical and biological contaminants, separate and contain the affected air, and filter out the contaminants. Technologies for verifying identities accurately and quickly help protect facilities from terrorist encroachment. Centrally administered hardware and software controls prevent cyber attacks and reduce the high costs of virus-infected computers.

Management Practices

Building owners and managers can also use management practices to reduce their risk from terrorism. Management practices can be procedural or technical. Some relate to security, training, communications, and emergency response. Others relate to location of and access to the building and systems and subsystems within the building. Some practices complement engineering alternatives, and others substitute for them.

Security practices are the use of security personnel and procedures to detect, deter, and prevent terrorist breaches and to capture attackers if a breach occurs. Security personnel may be used to perform identification checks at building entrances, conduct background checks on individuals with access to sensitive areas and information, patrol facilities, and monitor closed circuit TVs. Security strategies may also include use of biometric devices to verify identities and use of animals or sensors to detect dangerous materials and substances.

Emergency preparations reduce terrorist risk by improving survival or expediting recovery. Preparations to improve survival include establishing evacuation assembly or shelter areas, appointing evacuation coordinators, stockpiling essential supplies and provisions in shelters, and ensuring redundant electrical and HVAC systems. Preparations to expedite recovery include system redundancies, data backups, and remote facilities.

Training strategies are used primarily to prepare building occupants, owners and managers, and security and maintenance personnel to respond to terrorist breaches. Building occupants may receive training about evacuation routes or sheltering procedures to improve survival during emergencies [6]. Building owners and managers may institute regular emergency response drills for building occupants. Security and maintenance personnel may receive training about proper techniques for responding to incidents and containing damage. Training may also be used for prevention: building security personnel and occupants may be trained in detection of suspicious activities and notification procedures.

Building owners and managers can develop communications strategies to coordinate responses with emergency personnel and to relay information and instructions to occupants during emergencies. Communications strategies include setting up emergency phone numbers or instituting audio or e-mail broadcast mechanisms. Coordinated communications can play a key role in occupant safety. For example, after the North Tower of the World Trade Center was struck, there was confusion in the South Tower about whether to evacuate. This confusion led some occupants of upper floors who began to descend the stairs to return to their offices [10]. Building owners and managers can develop communications strategies to coordinate with first responders, security staff, and other emergency personnel responding to the incident. Finally, communications strategies can be used by firms occupying the building to facilitate recovery, assess consequences, and minimize disruptions to business.

Building structure-related management practices include location decisions for new construction (or new acquisitions), access to the building, and designation of its sensitive areas. New facilities are being designed and sited with protection in mind. Many government buildings have ample setbacks from roadways to prevent the delivery of bombs by vehicles. Designing and building appurtenant structures surrounding office buildings help preclude terrorists from reaching the intended target. Resiting existing embassies and siting new embassies in rural areas instead of busy urban areas also enhance security.

Financial Mechanisms

Building owners and managers can use financial mechanisms to reduce risk of terrorism-related losses. Two types of financial mechanisms that affect risk mitigation decisions are risk reduction through insurance and financial incentives.

Building owners and managers may choose to reduce their risk exposure to disasters by purchasing insurance for worker's compensation, property damage, business interruptions, event cancellation, and liability. Insurance does reduce the financial exposure of owners of constructed facilities to terrorist attacks by transferring the costs of an attack to other parties (i.e., insurance and reinsurance companies). It does not reduce the injuries to occupants and damages to property in the event of an attack.

Financial incentives encourage decision makers to make certain choices over others. In the case of risk mitigation, they are policies, measures, or characteristics that provide further financial motivation for building owners and facility managers to implement risk mitigation measures in their buildings. Financial incentives fall into two categories: public policy-based (government provided) incentives and market-based incentives.

The government can institute direct incentives that reduce the relative price that building owners and managers pay to protect their buildings. These incentives include subsidies, tax write-offs, cost sharing, or loan guarantees for investments in protective measures. Market-based incentives come from many sources. Insurers, for example, may lower terrorism insurance premiums for protected buildings if they expect reduced insurance claims following a terrorist incident. Tenants may value safety features of a building and be willing to pay a leasing premium. Protective investments in a building are improvements that may increase the value of the asset. The building owner would realize the benefit of this increase in property value when the property is turned over or when it is used as collateral for other transactions.

Economic Evaluation

Economic tools-evaluation methods and software for implementing the methods are needed to help decision makers invest in mitigation strategies that will provide the most cost-effective reduction in personal injuries, financial losses, and damages to constructed facilities.

This section demonstrates how to implement the third step in the protocol for developing a risk mitigation plan (i.e., how to apply life-cycle cost (LCC) analysis to choose among competing mitigation strategies). LCC analysis is a widely used method for conducting economic evaluations in constructed facilities; it is supported by the ASTM practice E 917 on LCC [1]. The LCC method measures in present value terms the sum of all relevant costs associated with owning, operating, and disposing of a constructed facility over a specified time period.

Information on cost items is needed in order to calculate life-cycle costs. Cost items are classified under two broad headings: (1) input costs and (2) event-related costs.

Input costs represent all costs tied to the building or facility under analysis that are not associated with an event. Input costs include the initial capital investment outlays for facilities and site work, future costs for electricity for lighting and space heating and cooling, future renovations, and any salvage value for plant and equipment remaining at the end of the study period.

Event-related costs are based on annual outcomes, each of which has a specified probability of occurrence. Each outcome has a set of cost items associated with it. The event modeling methodology is very flexible. For example, it can be used to model multiple hazards, such as those associated with earthquakes, high winds, or an accident resulting in widespread damage resulting from fire or chemical spills.

Once all costs have been identified and classified, year-by-year estimates are developed for each cost item for each alternative under analysis. These year-by-year estimates for each alternative are referred to as baseline values. The analysis using this "fixed set" of values is referred to as the baseline analysis. In this

article, the alternatives are as A_j (where the index for j ranges from 0,..., N, for a total of N+1 alternatives). For LCC evaluation to be valid, each A_j mitigation strategy must yield a minimum target level of protection benefits. Denote the alternative with the lowest initial investment cost as A_0; it is referred to as the base case. Some costs entering the analysis may be negative. For example, the resale of equipment and components at the end of the study period results in a salvage value whose present value equivalent is subtracted from investment costs.

The life-cycle costs of a given alternative, A_j, is denoted as LCC^j; it is expressed mathematically in equation 1 as:

$$LCC_j = \sum_{t=0}^{T} (I_{jt} + C_{jt} + E(L_{jt})/(1+d)^t \quad \text{(equation 1)}$$

where

- t = an index representing a unit of time;
- T = the length of the study period in years;
- d = the discount rate expressed as a decimal;
- I_{jt} = investment costs for alternative A_j in year t;
- C_{jt} = non-investment costs for alternative A_j in year t;
- $E(L_{jt})$ = expected value of losses for alternative A_j in year t.

The baseline analysis produces the calculated value of each alternative's life-cycle costs. The alternative with the lowest life-cycle cost is the most cost-effective alternative.

Once the most cost-effective alternative has been identified using best-guess estimates of uncertain values, "sensitivity analysis" enables the decision maker to evaluate the conditions under which other alternatives might result in lower life-cycle cost. The following case study illustrates both types of analysis.

1.a Significance of the Project:

The data center undergoing renovation is a single-story structure located in a suburban community. The floor area of the data center is 3,716 m^2 (40,000 ft^2). The replacement value of the data center is $20 million for the structure plus its contents. The data center contains financial records that are in constant use by the firm and its customers. Thus, any interruption of service will result in both lost revenues to the firm and potential financial hardship for the firm's customers. The occupants of the data center are part of the same parent company, but not part of the same corporate division responsible for facilities construction and renovation. The building owners employ two different renovation strategies. The first, referred to as the Base Case, employs upgrades which are consistent with pre-September 11th levels of security. Thus, the Base Case represents maintenance of the *status quo*. The second, referred to as the Proposed Alternative, recognizes that in the post-September 11th environment the data center faces heightened risks in two areas. These risks are associated with the vulnerability of information technology resources and the potential for damage to the facility and its contents from chemical, biological, radiological, and explosive (CBRE) hazards. Two scenarios—the potential for a cyber attack and the potential for a CBRE attack—are used to capture these risks.

1.b Key Points:

1. The objective of the renovation project is to provide cost-effective operations and security protection for the data center.
2. The renovation has been planned for some time to upgrade the data center's HVAC, telecommunications and data processing systems and to address a number of generic security concerns.
3. Two upgrade alternatives are proposed:
   - Base Case (Basic Renovation) and
   - Proposed Alternative (Enhanced Renovation), which augments the Base Case by strengthening portions of the exterior envelope, limiting vehicle access to the data center site, significantly improving the building's HVAC, data processing and telecommunications systems, and providing better linkage of security personnel to the telecommunications network.

2. Analysis Strategy: How Key Measures are Estimated

The following economic measures are calculated as present-value (PV) amounts:

(1) **Life-Cycle Costs** (LCC) for the Base Case (Basic Renovation) and for the Proposed Alternative (Enhanced Renovation), including all costs of acquiring and operating the data center over the length of the study period. The selection criterion is lowest LCC.

(2) **Present Value Net Savings** (PVNS) that will result from selecting the lowest-LCC alternative. PVNS > 0 indicates an economically worthwhile project.

Data and Assumptions:

- The Base Date is 2003.
- The alternative with the lower first cost (Basic Renovation) is designated the Base Case.
- The study period is 25 years and ends in 2027.
- The discount or hurdle rate is a 4.0 % real rate.
- Annual probabilities for the outcomes for each attack scenario are given along with outcome costs.
- Both the Base Case and the Proposed Alternative have similar types of outcome costs. Should a cyber attack occur, it results in damage to financial records and identity theft for a small set of corporate customers. Should a CBRE attack occur, it results in several non-fatal injuries, physical damage to the data center, interruption of business services at the data center, and denial of service to corporate customers during recovery.

Table 4— Summary of a Data Center Case Study

Case Study

3.a Calculation of Savings, Costs, and Additional Measures

Savings and Costs in Thousands of Dollars ($K)

PV of Investment Costs	**Base Case**	**Proposed Alt.**
Capital Investment	$1,168K	$1,772K
PV of Increased Investment Costs for Proposed Alt.		$604K
PV of Non-Investment Costs	**Base Case**	**Proposed Alt.**
O&M Costs	4,082K	3,201K
Other Costs	687K	282K
	$4,769K	$3,483K
PV of Non-Investment Savings for Proposed Alt.		$1,286K
LCC	**Base Case**	**Proposed Alt.**
PV of Investment Costs	1,168K	1,772K
PV of Non-Investment Costs	4,769K	3,483K
	$5,937K	$5,255K
PVNS from Proposed Alternative		**$682K**

3.b Key Results:

- **LCC**
  Base Case $5,937K
  Proposed Alt. $5,255K
- **PVNS from Alt.** $682K

3.c Traceability:

- Life-cycle costs were calculated according to ASTM Standard E 917.

Table 4 Continued — Summary of a Data Case Study

The data center case study illustrates an economic evaluation of an actual building renovation project. The case study [3] focuses exclusively on two of the three types of mitigation strategies-engineering alternatives and management practices for protection against terrorism.

Senior management is considering two alternative renovation strategies. The base case renovation has an initial investment cost of $1,100K; the enhanced renovation, designated as the proposed alternative, has an initial investment cost of $1,750K. The strategy that results in the lower life-cycle cost will be the recommended alternative.

Two types of analyses are used to evaluate the merits of the proposed alternative vis-à-vis the base case. First, a baseline analysis is performed in which all values are fixed. Second, a sensitivity analysis based on Monte Carlo simulation is performed in which 21 key input variables are allowed to vary in combination according to an experimental design.

Table 4 summarizes the baseline analysis. It provides a brief description of each renovation strategy and covers the background, approach, and results of the economic evaluation. Based on the summary format described in *ASTM Standard Guide E 2204* [2], the material presented in Table 4 provides a concise statement of why the proposed alternative is the "preferred" choice with a PVNS of $682K.

Life-cycle cost results of the sensitivity analysis are shown graphically in Figure 2. The life-cycle costs of the base case (LCC_{BC}) are compared to those of the proposed alternative (LCC_{Alt}). The results of the Monte Carlo simulation produced 1,000 observations of LCC_{BC} and 1,000 observations of LCC_{ALT}. These observations were used to produce the two traces shown in Figure 2. The figure was constructed by first sorting the values of LCC_{BC} and LCC_{Alt} from smallest to largest. The resultant cumulative distribution function was then plotted. The vertical axis records the probability that the economic measure-LCC_{BC} or LCC_{Alt}—is less than or equal to a specified value. The values recorded on the horizontal axis cover the range of LCC values encountered during the Monte Carlo simulation.

In analyzing Figure 2, note that the values of LCC_{BC} and LCC_{Alt} from the baseline analysis were $5,937K and $5,255K, respectively. The life-cycle cost trace of the proposed alternative in Figure 2 always remains to the left of the life-cycle cost trace of the base case. Thus, for any given probability (e.g., 0.40), the life-cycle cost of the proposed alternative ($5,000K) is less than the life-cycle cost of the base case ($5,600K). Similarly, for any given life-cycle cost (e.g., $5,000K), the probability of being less than or equal to that cost is higher for the proposed alternative (0.40) than for the base case (0.23). Also, the horizontal distance between the proposed alternative and the base case gets larger as the cumulative probability moves from 0.00 to 1.00. This translates into a wider range of life-cycle costs for the base case (i.e., maximum minus minimum). Figure 8-1 clearly demonstrates that the proposed alternative is the more cost-effective renovation strategy.

Future Research

Decision makers need help in determining what strategies are most cost effective in protecting constructed facilities against natural and man-made hazards. This article presents a three-step protocol for determining facility vulnerability and making economic choices among strategies.

The third step in the protocol requires the user to generate a LCC measure of economic merit using equation 1. This requires collecting the appropriate cost figures, making appropriate assumptions about the study period and discount rate, and calculating correctly the LCC values for base case and proposed alternatives. Many decision makers will not be familiar with such analyses, however, and will find them difficult to perform.

A software tool is needed that helps decision makers collect the right data, make appropriate assumptions, execute error-free calculations, perform sensitivity analysis, and report the relative economic merits of protection strategies in a standard format. The National Institute of Standards and Technology is currently developing such a software tool and plans to have it available for Beta testing in September 2004 and for general use early in 2005.

REFERENCES

1. ASTM International. 2002. "*Standard Practice for Measuring Life-Cycle Costs of Buildings and Building Systems.*" E 917. **Annual Book of ASTM Standards: 2002**. Vol. 04.11. West Conshohocken, PA: ASTM International.

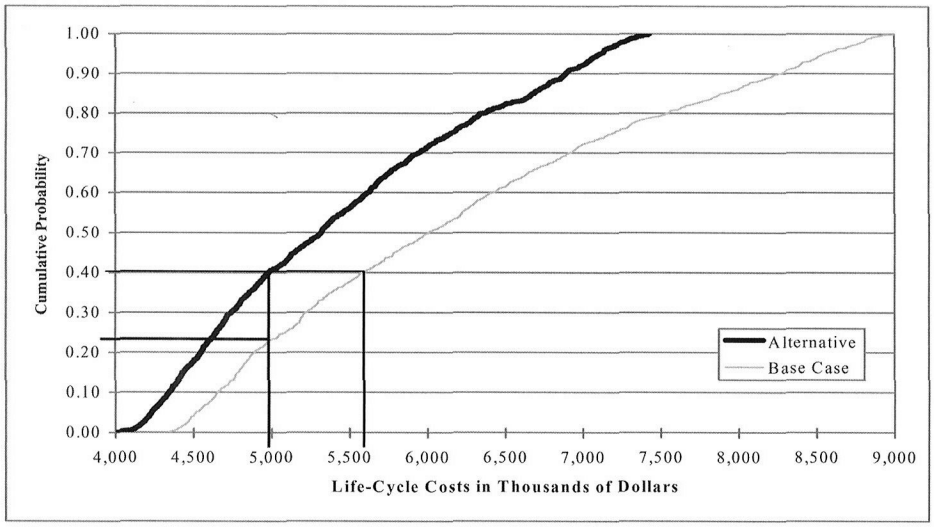

Figure 2 — Life-Cycle Costs for Each Alternative in Thousands of Dollars Resulting from Changes in All of the Variables

2. ASTM International. 2002. "*Standard Guide for Summarizing the Economic Impacts of Building Related Projects.*" E2204. **Annual Book of ASTM Standards: 2002**. Vol. 04.11. West Conshohocken, PA: ASTM International.
3. Chapman, Robert E., *Applications of Life-Cycle Cost Analysis to Homeland Security Issues in Constructed Facilities: A Case Study*, NISTIR 7025, (Gaithersburg, MD: National Institute of Standards and Technology, October 2003).
4. Dols, W. Stuart and George N. Walton, "*CONTAMW 2.0*," documented in CONTAMW 2.0 User Manual Multizone Airflow and Contaminant Transport Analysis Software, NISTIR 6921, (Gaithersburg, MD: National Institute of Standards and Technology, November 2002). Available at: http://www.bfrl.nist.gov/IAQanalysis/CONTAMWdesc.htm
5. Hartwig, Robert, "*The Long Shadow of September 11: Terrorism and Its Impacts on Insurance and Reinsurance Markets.*" (Insurance Information Institute: July 2002). Available at: http://www.iii.org/media/hottopics/insurance/sept11/
6. Hays, Constance L., "*As Important as the Corporate Disaster Plan Is How Fast the Employees Carry It Out,*" New York Times, September 12, 2001, pp C10.
7. Hunter, Regina L. "*Risk Assessment Method--Property Analysis and Ranking Tool: Risk Analysis Software for the GSA Property Manager,*" mimeo, Sandia National Laboratories (2001).
8. Karter, Michael J., Jr., **NFPA Journal**, Volumes 84-95, No. 5 (September/October 1990-2001).
9. Lewis, Bernard T. and Richard P. Payant. **The Facility Manager's Emergency Preparedness Handbook** (New York: AMACOM Books, 2003).
10. Moss, Michael and Bagli, Charles V., "*Instincts to Flee Competed With Instructions to Remain,*" New York Times, September 13, 2001, pp. A6.
11. Owen, David D. and R.S. Means Engineering Staff. **Building Security: Strategies & Costs** (Kingston, Massachusetts: Construction Publishers & Consultants, 2003).
12. U.S. Chemical Safety and Hazard Investigation Board, Chemical Incidents Reports Center, "*CSB Incident News Reports,*" August 2003. Available at: http://www.chemsafety.gov/circ
13. U.S. Department of Defense, *DOD Minimum Antiterrorism Standards for Buildings*, UFC 4-010-01, (Washington, DC: July 2002). Available at: http://www.hnd.usace.army.mil/techinfo/ufc/ufc4-010-01.pdf
14. U.S. Department of Homeland Security, *Integrating Human-Caused Hazards Into Mitigation Planning, FEMA 386-7.* (Federal Emergency Management Agency: August 2001). Available at: http://www.fema.gov/fima/planning_toc3.shtm
15. U.S. Department of Homeland Security, *Understanding Your Risks - Identifying Hazards and Estimating Losses, FEMA 386-2.* (Federal Emergency Management Agency: August 2001). Available at: http://www.fema.gov/fima/planning_toc3.shtm
16. U.S. Department of State, "*Significant Terrorist Incidents 1961-2001: A Brief Chronology,*" (Office of the Historian, Bureau of Public Affairs: September 28, 2001). Available at: http://www.state.gov/r/pa/ho/pubs/fs/5902.htm

ABOUT THE AUTHORS

Dr. Harold E. Marshall is chief of the Office of Applied Economics with the National Institute of Standards and Technology at Gaithersburg, MD. He can be contacted by sending e-mail to harold.marshall@nist.gov. Robert E. Chapman and Chi J. Leng are associates of Dr. Marshall.

Technical Articles - Each month, **Cost Engineering** journal publishes one or more peer-reviewed technical articles. These articles go through a blind peer review evaluation prior to publication. Experts in the subject area judge the technical accuracy of the articles. They advise the authors on the strengths and weaknesses of their submissions and what changes can be made to improve the article.