Report Documentation Page

Form Approved
OMB No. 0704-0188

1. REPORT DATE	2. REPORT TYPE	3. DATES COVERED
2007	**final**	**00-00-2007 to 00-00-2007**

4. TITLE AND SUBTITLE	5a. CONTRACT NUMBER
Securing America's passenger-rail systems	5b. GRANT NUMBER
	5c. PROGRAM ELEMENT NUMBER
6. AUTHOR(S)	5d. PROJECT NUMBER
Jeremy Wilson; Brian Jackson; Mel Eisman; Paul Steinberg; Kevin Riley	5e. TASK NUMBER
	5f. WORK UNIT NUMBER
7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES)	8. PERFORMING ORGANIZATION REPORT NUMBER
RAND Corporation,1776 Main Street,Santa Monica,CA,90401-3208	**RAND/MG-705-NIJ**
9. SPONSORING/MONITORING AGENCY NAME(S) AND ADDRESS(ES)	10. SPONSOR/MONITOR'S ACRONYM(S)
Captain James Malcom, HQ USAF/A8XP, Room 4D1083, 1070 Air Force Pentagon, Washington, DC, 20330-1070	11. SPONSOR/MONITOR'S REPORT NUMBER(S)

12. DISTRIBUTION/AVAILABILITY STATEMENT

Approved for public release; distribution unlimited

13. SUPPLEMENTARY NOTES

Online access http://www.rand.org/pubs/monographs/MG705/

14. ABSTRACT

U.S. communities depend on reliable, safe, and secure rail systems. Each weekday, more than 12 million passengers take to U.S. railways. Recent attacks on passenger-rail systems around the world highlight the vulnerability of rail travel and the importance of rail security for these passengers. The use of passenger rail and the frequency with which terrorists target it call for a commitment to analyzing and improving rail security in the United States. This book explains a framework for security planners and policymakers to use to guide cost-effective rail-security planning, specifically for the risk of terrorism. Risk is a function of threat (presence of terrorists with intent, weapons, and capability to attack), vulnerability (likelihood of damage at a target, given an attack), and consequences (nature and scale of damages if an attack succeeds). While effective security solutions may address all three components of risk, this book focuses on addressing vulnerabilities and limiting consequences, since these are the two components of risk most within the realm of rail-security personnel. The analysis is based on a notional rail system that characterizes rail systems typically found in the United States. The methodology presented is useful for planning rail-security options.

15. SUBJECT TERMS

16. SECURITY CLASSIFICATION OF:			17. LIMITATION OF ABSTRACT	18. NUMBER OF PAGES	19a. NAME OF RESPONSIBLE PERSON
a. REPORT	b. ABSTRACT	c. THIS PAGE			
unclassified	**unclassified**	**unclassified**	**Same as Report (SAR)**	**142**	

This product is part of the RAND Corporation monograph series. RAND monographs present major research findings that address the challenges facing the public and private sectors. All RAND monographs undergo rigorous peer review to ensure high standards for research quality and objectivity.

Securing America's Passenger-Rail Systems

Jeremy M. Wilson, Brian A. Jackson, Mel Eisman,
Paul Steinberg, K. Jack Riley

Supported by the National Institute of Justice

Homeland Security

A RAND INFRASTRUCTURE, SAFETY, AND ENVIRONMENT PROGRAM

The research described in this report was supported by the National Institute of Justice, Office of Justice Programs, U.S. Department of Justice and was conducted under the auspices of the Homeland Security Program within RAND Infrastructure, Safety, and Evironment. The opinions, findings, and conclusions or recommendations expressed in this publication are those of the authors and do not necessarily reflect the views of the Department of Justice.

Library of Congress Cataloging-in-Publication Data

Securing America's passenger-rail systems / Jeremy M. Wilson ... [et al.].
p. cm.
Includes bibliographical references.
ISBN 978-0-8330-4117-3 (pbk. : alk. paper)
1. Railroads—United States—Passenger traffic. 2. Transportation—United States—Passenger traffic. I. Wilson, Jeremy M., 1974–

TF23.S43 2008
363.28'74—dc22

2007048795

Published 2007 by the RAND Corporation
1776 Main Street, P.O. Box 2138, Santa Monica, CA 90407-2138
1200 South Hayes Street, Arlington, VA 22202-5050
4570 Fifth Avenue, Suite 600, Pittsburgh, PA 15213-2665
RAND URL: http://www.rand.org
To order RAND documents or to obtain additional information, contact
Distribution Services: Telephone: (310) 451-7002;
Fax: (310) 451-6915; Email: order@rand.org

Preface

Communities across the United States rely on reliable, safe, and secure rail systems. Each weekday, more than 12 million passengers take to U.S. railways. Recent attacks on passenger-rail systems around the world highlight the vulnerability of this form of transportation. The high use of passenger rail and the frequency with which terrorists target rail systems elsewhere call for a commitment to analyzing and improving rail security in the United States.

The study on which this book reports represented a step in that direction by providing a framework that security planners and policymakers can use to prepare for, and protect against, threats to and vulnerabilities of rail systems. The analyses that emerge from using the framework are general enough to allow the work to be made publicly available but specific enough to provide guidance from the national level all the way down to the individual rail systems. These qualities, combined with this book's synthesis of issues related to both rail-system vulnerabilities and how to cost-effectively reduce them, contribute to its broad applicability and utility for those working to improve rail security. The intended audience of this book includes security planners—both experts working directly within rail systems and those who facilitate rail security through their work in governmental or professional organizations—and policymakers. However, researchers may also be interested in the substantive discussions about terrorism and methodology.

Those who are interested in this book may also be interested in some of RAND's other recent studies that relate to security, including the following:

- *Implementing Security Improvement Options at Los Angeles International Airport* (Stevens, Hamilton, et al., 2006)
- *Near-Term Options for Improving Security at Los Angeles International Airport* (Stevens, Schell, et al., 2004)
- *Reducing Terrorism Risk at Shopping Centers: An Analysis of Potential Security Options* (LaTourrette et al., 2006)
- *Protecting Commercial Aviation Against the Shoulder-Fired Missile Threat* (Chow et al., 2005)

- *Breaching the Fortress Wall: Understanding Terrorist Efforts to Overcome Defensive Technologies* (Jackson, Chalk, et al., 2007)
- *Aptitude for Destruction*, Vol. 1: *Organizational Learning in Terrorist Groups and Its Implications for Combating Terrorism* (Jackson, Baker, et al., 2005)
- *Estimating Terrorism Risk* (Willis et al., 2005)
- *Exploring Terrorist Targeting Preferences* (Libicki, Chalk, and Sisson, 2007).

This project was supported by the National Institute of Justice, Office of Justice Programs, U.S. Department of Justice. The opinions, findings, and conclusions or recommendations expressed in this publication are those of the authors and do not necessarily reflect the views of the Department of Justice.

The RAND Homeland Security Program

This research was conducted under the auspices of the Homeland Security Program within RAND Infrastructure, Safety, and Environment (ISE). The mission of ISE is to improve the development, operation, use, and protection of society's essential physical assets and natural resources and to enhance the related social assets of safety and security of individuals in transit and in their workplaces and communities. Homeland Security Program research supports the U.S. Department of Homeland Security and other agencies charged with preventing and mitigating the effects of terrorist activity within U.S. borders. Projects address critical infrastructure protection, emergency management, terrorism risk management, border control, first responders and preparedness, domestic threat assessments, domestic intelligence, and workforce and training.

Questions or comments about this monograph should be sent to the project leader, Jeremy Wilson (Jeremy_Wilson@rand.org). Information about the Homeland Security Program is available online (http://www.rand.org/ise/security/). Inquiries about homeland security research projects should be sent to the following address:

Andrew Morral, Director
Homeland Security Program, ISE
RAND Corporation
1200 South Hayes Street
Arlington, VA 22202-5050
703-413-1100, x5119
Andrew_Morral@rand.org

Contents

Preface iii
Figures vii
Tables ix
Summary xi
Acknowledgments xvii
Abbreviations xix

CHAPTER ONE
Introduction 1
Background 1
Objectives and Scope 3
Approach 4
Outline of Book 5

CHAPTER TWO
What Are the Key Rail-Attack Threats and Their Consequences? 7
Introduction 7
Weapons and Tactics Used Against Rail Systems 8
The Targets of Terrorist Attacks in Rail Systems 10
Outcomes of Past Terrorist Attacks on Rail Systems 12
Lessons from the Threat Assessment 16

CHAPTER THREE
Qualitative Risk Assessment for a Notional Passenger-Rail System 17
Introduction 17
Laying Out a Notional Rail System 17
Determining Attack Scenarios 18
Qualitatively Assessing Terrorism Risk 20

CHAPTER FOUR
Baseline Security and Operational Characteristics of the Notional Rail System 25
Introduction 25

Defining the Baseline Security Measures 26
Notional Rail System Description 27
Defining Security Layers for the Notional Rail System 29

CHAPTER FIVE
Cost-Effectiveness Assessment of Security-Improvement Options for the Notional Rail System 33
Introduction 33
Assessment-Process Overview 34
Characterizing and Estimating Costs of Security-Improvement Options 36
Process-Based Security-Improvement Options: Implementing Enhanced Security Training 38
Technology-Based Security-Improvement Options: Installing Perimeter Fencing and Intrusion-Detection Systems Adjacent to Ground-Level Tracks 38
Infrastructure- or Facility-Modification Security-Improvement Options: Installing Blast-Resistant Containers in Stations 39
Perimeter-Layer Cost-Effectiveness Assessment Process 39
Prioritize Attack Scenarios by Level of Assessed Risk 39
Assess Relative Effectiveness of Security-Improvement Options 41
Combine Effectiveness Assessments with Costs 61
Generate Preferred List of Security-Improvement Options at the Perimeter Layer 61
Test the Robustness of the Overall Cost-Effectiveness Process 64
Assess Security-Improvement Options Across All Layers and Generate System-Level Recommendations 67
Deal with Economic and Budgetary Limitations 70
Recognize Interdependence Across Security Options 70
Ensure a Proper Balance of Security-Improvement Options 72
Assess Timelines for Implementing Security-Improvement Options 72
Limitations on Using the Analytical Assessment Process 73

CHAPTER SIX
Rail-Security Policy Considerations 77
Rail-Security Lessons at the System Level 77
The Future of Rail Security 79
Rail Security Versus the Security of Everything Else 81
Conclusions 82

APPENDIXES
A. Qualitative Risk Assessment of Rail-Attack Scenarios 85
B. Cost-Effectiveness Assessment Details 97

References 117

Figures

2.1. Locations of and Tactics Used for Rail Attacks 11
2.2. Average Fatalities and Injuries Resulting from Attacks on Rail Systems, Overall and by Location of Attack 13
2.3. Distributions of Fatalities and Injuries in Attacks on Rail Systems 14
3.1. The Rail System as a Terrorist Target: A Notional System 18
3.2. Summary of Qualitative Terrorism-Risk Levels Associated with Different Terrorist Attack Scenarios 23
4.1. The Notional Passenger-Rail System Network 28
4.2. Potential Terrorist-Attack Targets 30
5.1. Cost-Effectiveness Assessment Process 34
5.2. Notional Rail-System Network and Potential Perimeter Target Locations 56
5.3. Example of Interdependence of Security Measures for Access-Control Systems 71
5.4. The Notional Passenger-Rail System and Potential Changes to It 74
A.1. Qualitative Threat of Specific Rail-System Attack Scenarios 87
A.2. Qualitative Vulnerability of Rail-System Components to Specific Attack Scenarios 88
A.3. Consequence-Categorization Matrix for Attack Modes and Locations 89
A.4. Casualty-Consequence Categorization Matrix 91
A.5. Overall Potential-Consequence Ranking for Attack Scenarios, Based on Casualty Expectations 92
A.6. Overall Potential-Consequence Ranking for Attack Scenarios, Based on Economic Expectations 93
A.7. Total Net Consequence Categorization Matrix 93
A.8. Overall Total Net Potential-Consequence Ranking for Attack Modes at Specific Rail-System Locations 94
A.9. Threat-Vulnerability Categorization Matrix 95
A.10. Composite Threat-Vulnerability Rankings for Attack Modes at Specific Locations in a Notional Rail System 95
A.11. Threat-Vulnerability-Consequence Categorization Matrix 96
A.12. Composite Qualitative Risk Rankings for Attack Modes at Specific Locations in a Notional Rail System 96
B.1. Estimate of Tolerance to Direct Effects of Air Blast 112

B.2. Lethality of Small Explosives 113
B.3. Representative Blast Damage 113
B.4. Cumulative Cost-Effectiveness of Perimeter-Layer Security-Improvement Options 115

Tables

2.1. Terrorist Tactics in Rail Incidents 9
2.2. Weapons Used in Rail Incidents 10
2.3. Injuries and Fatalities in Rail Incidents, by Terrorist Tactic 15
4.1. Potential Target Locations Across Layered Security Areas 31
5.1. Comparisons of Security-Improvement Option Types 36
5.2. Marginal Costs of Three Sets of Security-Improvement Options 37
5.3. Risk-Assessment Summary Across Perimeter Locations 40
5.4. Assessment of Perimeter Security-Improvement Options Preventing Terrorist Attacks from Occurring 44
5.5. Perimeter Security-Improvement Option Assessment Ratings for Preventing Terrorist Attacks from Occurring 45
5.6. Benchmark Magnitude of Fatalities Assessed Across the Perimeter Layer 47
5.7. Assessment of Perimeter Security-Improvement Option Effectiveness in Averting Fatalities 49
5.8. Benchmark Recovery Times (Days), Estimated Across the Perimeter Layer 52
5.9. Assessment of Perimeter Security-Improvement Option Effectiveness in Reducing Recovery Times 54
5.10. Benchmark Loss of Operating Revenues ($ million), Estimated Across the Perimeter 57
5.11. Assessment of Perimeter Security-Improvement Option Effectiveness in Reducing Operating-Revenue Losses 59
5.12. Perimeter-Layer Effectiveness-Assessment Summary Results 62
5.13. Perimeter-Layer Security-Improvement Option Effectiveness and Cost Summary 63
5.14. Preferred Security-Improvement Options for the Perimeter Layer 64
5.15. Preferred Security-Improvement Options Across Five Security Layers 68
5.16. System-Level Security-Improvement Recommendations 69
A.1. Threat Ranking of Attack Modes 86
A.2. Potential-Consequence Ranking of Attack Modes 90
A.3. Potential-Consequence Ranking of Attack Locations 91

Summary

Introduction

Communities across the United States rely on reliable, safe, and secure rail systems. Each weekday, more than 12 million passengers take to U.S. railways. Recent attacks on passenger-rail systems around the world highlight the vulnerability of rail travel and the importance of rail security for these passengers. Even though there have been no successful attacks on rail systems in the United States recently, the FBI and local police departments have thwarted several planned attacks against the New York subway system alone. The use of passenger rail and the frequency with which terrorists target it call for a commitment to analyzing and improving rail security in the United States.

The goal of the study on which this book reports was to develop a framework for security planners and policymakers that can be used to guide cost-effective rail-security planning. The security analyzed in this book specifically addresses the risk of terrorism. As described more fully in Chapter Three, risk is a function of threat (presence of terrorists with intent, weapons, and capability to attack), vulnerability (likelihood of damage at a target, given an attack), and consequences (nature and scale of damage if an attack succeeds). While effective security solutions may address all three components of risk, this book focuses on addressing vulnerabilities and limiting consequences, since these are the two components of risk most within the realm of rail-security personnel. The study focused on passenger, as opposed to freight, rail systems. Because of the tremendous variation in the types of rail systems and the desire not to reveal the specific security measures of any one rail system, the analysis is based on a notional rail system that characterizes rail systems typically found in the United States.

Rail-Attack Threats

Drawing primarily on available data on past terrorist attacks on rail systems from the RAND-MIPT Terrorism Incident Database (National Memorial Institute for the Prevention of Terrorism and RAND Corporation, ongoing), we found that the most

prevalent terrorist threat to rail systems comes from bombings, that most terrorist attacks on rail systems produce few fatalities and injuries, and that attacks in densely packed rail cars and interior rail-facility locations are of particular concern because of the casualties they can produce. Not all terrorist attacks on rail systems come from explosives, so security measures must address explosive devices but also appropriately incorporate the possibility of rarer attack modes. In addition, given the damage associated with a relatively small number of large attacks, security measures that prevent only the largest-scale attacks could significantly reduce the human costs associated with this threat.

Although historical data and the patterns of behavior they document provide a foundation for security decisionmaking today, it must be emphasized that terrorists are dynamic adversaries whose attack patterns may change in response to security measures. Security portfolios, thus, should not be static defenses, but rather should be reviewed periodically to ensure that they remain relevant to any changes in terrorists' targeting methods.

Passenger Rail and Terrorism Risk

To understand the vulnerability of rail systems to the terrorist threat, we constructed a notional—or hypothetical—rail system. We then subjected that notional system to a range of attack scenarios to identify the specific set of attacks to which the rail system was most at risk. The threat scenarios were drawn from past attack reports and other open-source information.

The vulnerability assessment identified 11 potential target locations (e.g., system-operation and power infrastructure) within a notional rail system and eight potential attack modes (e.g., small explosives). These targets and attack modes were combined to produce 88 different *attack scenarios* of concern. Each scenario was then categorized high, medium, low, or no risk.[1] The categorization represents qualitative judgments about terrorists' ability to exploit the vulnerability and the consequences if they were to succeed.

Baseline Security and Operational Characteristics of the Notional Rail System

The end objective is to identify *additional increments* to security that can be implemented in a cost-effective manner. However, all rail systems have at least some security measures in place, and those security measures, in turn, have some impact. Thus, we

[1] The no-risk categorization results when the attack-target combination is not possible.

had to further specify our notional rail system by describing the existing baseline security system and its effectiveness.

We assumed a relatively simple notional rail network located within a major metropolitan area, consisting of five spokes of unique rail lines going directly into one hub central station, with the only transfer point between these lines located at the hub station. We further assumed that the baseline notional rail-security system would have the following security measures in place: perimeter and station surveillance systems,[2] uniformed patrols, available rapid-deployment forces, and an automated vehicle locator (AVL) system (assumed to be located at the operation-control center) for detecting unusual delays in trains within any one of the many lines within the notional rail system.

In addition, we adopted the vision of a multilayered transportation security system illustrated in a recent Federal Transit Administration report (Rabkin et al., 2004), in which we defined each layer as going from first safeguarding the outermost *perimeter* to the *exterior, interior*, and *restricted access* areas to the innermost rail security *asset*, the trains.

Cost-Effective Security-Improvement Options for the Notional Rail System

With the notional system's existing security defined, we could then turn our attention to what improvements to that security could be made. We identified 17 security-improvement options (SIOs) within three broad categories: (1) process-based improvements (e.g., implementing enhanced security training), (2) technology-based alternatives (e.g., using portable [handheld] detection systems), and (3) infrastructure and facility modifications (e.g., installing blast-resistant containers).

We assessed the relative effectiveness of the 17 SIOs across the five security layers laid out above. We evaluate effectiveness by assessing the SIO's performance against four criteria: (1) preventing or reducing the probability of a specific terrorist attack occurring, (2) reducing or averting the number of fatalities of passengers in the system, (3) reducing the time necessary for system facilities and infrastructure to be restored and operations fully resumed, and (4) minimizing rail operating-revenue losses. The 17 security measures were rated for their incremental impact at each layer, as well as to their potential system-level contribution across layers.

At the system level (integrating across layers), we identified four broad categories of cost-effective security measures for system operators to consider: (1) relatively inexpensive solutions with the highest effectiveness-per-dollar metric payoffs (e.g., enhanced

[2] The baseline surveillance system is a limited system comprised of CCTV cameras installed at the entrances and exits and within the infrastructure, concourse areas, corridors, escalators, and other passages leading to the train platforms.

security training), (2) additional inexpensive solutions to consider with reasonable levels of effectiveness-per-dollar metric payoffs (e.g., installing retractable bollards at entrances and exits of the operation-control center and power plant), (3) costlier solutions with highest effectiveness-per-dollar metric payoffs (e.g., installing fixed barriers at curbsides adjacent to all entrances and passageways leading to ground-level and underground stations), and (4) relatively expensive, longer-term solutions for future consideration (e.g., rail-vehicle surveillance systems). For our notional system, even though we prioritized the mix of security measures relative to affordability, the actual list of recommendations could depend on a variety of practical constraints, concerns, or needs, such as the ease and speed of implementation or budget constraints relative to other rail-system expansion plans, which we identify in this book.

Rail-Security Policy Considerations

Given the open and accessible characteristics of rail systems, the unpredictability of terrorist attacks, the continual evolution of risk as terrorists learn and improve their capabilities, and finite resources for security provision, the United States faces a complex security problem that has existed for decades. This book illustrates a process—a framework and a broad range of management considerations—for thinking through how to systematically improve the security of U.S. passenger systems to help ensure maximum protection at the lowest cost.

Rail-Security Lessons at the System Level

Security planners can draw from the framework and analysis described here to structure their security-improvement efforts. The process begins with conducting a detailed vulnerability assessment. Once the system's vulnerabilities are understood, potential increments or additions to existing security measures can be identified.

As the security posture of a specific rail system is examined, two factors must be kept in mind. First, security measures designed to thwart terrorism may have an added impact on preventing and mitigating ordinary crime or may have to be scaled up to address crime-related issues. Thus, the security measures chosen may have broader costs and benefits than those relating only to terrorism. Second, terrorists may seek to overcome defensive measures. Thus, those in charge of acquiring security improvements must consider how terrorist groups might react to potential security-improvement defenses put in place, so that they can make informed investment decisions.

The Future of Rail Security

We have already witnessed some important changes in terrorist-attack patterns against transportation in the few short years since 9/11, including concerted efforts to develop

bombs that can evade airport detection equipment. Thus, we can predict with near certainty that terrorist-attack patterns will change in the future, though we cannot predict with much certainty precisely how those changes will be manifested. Given this uncertainty, rail-security systems must be designed to be responsive to potential changes in attack patterns, and the consequent impact on the relative effectiveness of the security portfolio must be reevaluated periodically.

Research and development in improving and maturing countermeasure technologies and investments in human capital are elements of developing and maintaining robust security measures. Improvements in the performance of these technologies can diminish the terrorists' ability to successfully attack and reduce the indirect costs of security operations, such as the time required to screen passengers and baggage. Though technologies can perform many security functions, the people who use and monitor them are frequently the most critical element of the overall security system, and there is no substitute for having highly responsive and skilled staff in the security loop. To maintain the performance of personnel at the highest readiness levels, managers will have to invest in both enhanced security training and field testing. The former ensures that the personnel are most adept at operating the latest technologies; the latter helps ensure that they are highly proficient in implementing the set of emergency-response protocols and procedures as needed.

Rail Security Versus the Security of Everything Else

A common response by terrorists to the deployment of security measures is simply to move attack operations away from the defended area to softer targets located elsewhere. If defenses are deployed in one rail system, this behavior could move risk from one site to another. Likewise, if rail-security measures are increased across the entire rail-transportation system, attacks may simply be displaced onto other targets, such as a shopping mall or sport stadium. Under some circumstances, displacement could be viewed as a favorable outcome, if, for example, the attack was displaced to a location that is much easier to respond to than the original target location would have been.

Given that security in one setting relates to security in another, federal policymakers ultimately must decide how best to allocate security dollars not only across rail systems but also across other modes of transportation, critical infrastructure, and public venues. We cannot, from this analysis, draw conclusions about whether authorities should spend more on rail and less on air-transportation security, because we did not conduct such cross-mode and cross-target comparisons. We can, however, point to the applicability of this assessment methodology to decisionmaking about allocating security resources generally. We strongly encourage analysts, scholars, and researchers to extend the application of this form of methodology to such critical resource-allocation problems.

Conclusions

It bears repeating that the prioritized SIOs identified in this book are specific to the notional system we analyzed. Furthermore, the analysis performed here captures a point in time—the attractiveness of different SIOs in our prioritization is driven by the current costs for those options and their current perceived effectiveness. As a result, even if the preferred SIOs described here are viewed as reasonable for a given system, even that conclusion is perishable.

These limitations notwithstanding, the methodology presented here is useful for planning rail-security options. The methodology should, however, be tested against other systems of varying complexity. Such testing will yield two insights. First, we will understand better whether the portfolio of preferred SIOs varies with system complexity or is largely the same regardless. Since both risk and the nature of preexisting security measures will vary by the type of system examined, such experimentation will also give some insight into the dynamic nature of the threat- and security-assessment processes and, perhaps, the timeline over which the assessments need to be repeated to counter the fact that terrorists wield new methods and learn potential targets' defenses over time. Second, applying the methodology to systems of differing complexity will allow us to better understand the information demands that the framework imposes. The methodology is most useful if the information it requires is relatively easily obtained in a consistent and comprehensive manner.

Acknowledgments

As with any large, complex analysis, many people offer meaningful contributions beyond those participating directly on the research team.

We would like to thank the National Institute of Justice for supporting this work. Greg Hull of the American Public Transportation Association was instrumental, providing both key contacts and useful background information. We also appreciate the inputs we received from the staff of the many organizations we interviewed, including the Association of American Railroads, American Public Transportation Association, British Transport Police, Metropolitan Police in London, London Underground, Los Angeles County Sheriff's Department, Metro de Madrid, Metropolitan Transportation Authority in New York City, New Jersey Transit, New York City Police Department, Port Authority of New York and New Jersey, Port Authority Trans-Hudson Corporation, San Francisco Municipal Transportation Agency, Policia Nacional (the Spanish national police), Red Nacional de Ferrocarriles Españoles (RENFE, Spain's national railway network), Administrador de Infraestructuras Ferroviarias (ADIF, Spain's administrator of railway infrastructure), UK Department for Transport, UK Home Office, UK Network Rail, UK Transport Salaried Staffs' Association, U.S. Department of Homeland Security, and Washington Metropolitan Area Transit Authority.

We also must thank those who provided direct research assistance, including Greg Hannah, who provided key support relative to our work in the United Kingdom; Brian Carroll and Melanie Sisson, who provided general support throughout the project; and Drew Curiel for his assistance with data extraction and analysis from the RAND-MIPT Terrorism Incident Database.

Finally, we must thank Tom LaTourrette, Adrian Dwyer, Genevieve Giuliano, and Mike Wermuth, who provided important feedback on drafts, and Lisa Bernard, who offered editorial assistance, all of whom helped to significantly increase the quality of the final manuscript.

Abbreviations

AAR	American Association of Railroads
ACS	access-control system
ADIF	Administrador de Infraestructuras Ferroviarias
Amtrak	National Railroad Passenger Corporation
APTA	American Public Transit Association
AVL	automated vehicle locator
BART	Bay Area Rapid Transit
BTP	British Transport Police
CNP	Cuerpo Nacional de Policia
CWA	chemical-warfare agent
DHS	U.S. Department of Homeland Security
DOT	U.S. Department of Transportation
ECD	electron-capture detector
FTA	Federal Transit Administration
G&T	Grants and Training
GAO	Government Accountability Office
IDS	intrusion-detection system
IED	improvised explosive device
IMS	ion-mobility spectrometry
IR	infrared

MARTA	Metropolitan Atlanta Rapid Transit Authority
MMW	millimeter wave
NYPD	New York City Police Department
PATH	Port Authority Trans-Hudson Corporation
PROTECT	Program of Response Options and Technology Enhancements for Chemical/Biological Terrorism
RENFE	Red Nacional de Ferrocarriles Españoles
ROM	rough order of magnitude
SAW	surface acoustic wave
SFMTA	San Francisco Municipal Transportation Agency
SIO	security-improvement option
SME	subject-matter expert
TIC	toxic industrial chemical
TRL	technology-readiness level
TSSA	Transport Salaried Staffs' Association
UASI	Urban Area Security Initiative
WMATA	Washington Metropolitan Area Transit Authority

CHAPTER ONE

Introduction

Background

In 2004, more than 534 million passengers took to U.S. rails (Boardman, 2005), making more than 3.5 billion trips (APTA, 2006).[1] And these estimates do not count the passengers traveling on the National Railroad Passenger Corporation (Amtrak) system, the primary intercity rail system in the United States, which totaled 25 million in fiscal year 2005 (Berrick, 2007). By comparison, as many people traverse New York's Penn Station in a single morning as travel through Chicago's O'Hare International Airport in about two and a half days (Freeman, 2005).

Unfortunately, recent attacks against rail and subway systems highlight the vulnerability of rail travel and the importance of rail security for these passengers. For example, in Delhi in February 2007, explosives in two suitcases on a train bound for Lahore killed at least 66 people and injured 13 others ("Leaders Condemn India Train Blast," 2007); in London in July 2005, three suicide bombers detonated bombs on the Underground subway system, killing 39 people and injuring more than 660.[2] And in Madrid in March 2004, 10 bombs were detonated on commuter trains during rush hour, killing 191 people and injuring more than 1,800. Although there have been no recent successful attacks on rail systems in the United States, the FBI and local police departments have thwarted several planned attacks against the New York subway system alone (e.g., Rashbaum, 2007; Associated Press, 2007; Wedge, 2006; Oren, Mazor, and Geller, 2006). In the past, terrorists have targeted rail systems to produce both economic damage (by damaging or disrupting the operation of the systems) and human casualties (by injuring or killing the passengers). As recent operations against these systems suggest, a central focus in contemporary terrorist targeting of these systems has been to produce large-scale, mass-casualty attacks.

Passenger-rail systems are particularly vulnerable for a number of reasons, many of which RAND authors and the U.S. Government Accountability Office (GAO) staff

[1] This includes commuter, heavy, and light rail systems.

[2] An additional suicide bomber detonated an explosive device on a double-decker bus, killing an additional 13 people and injuring more than 110 ("7 July Bombings," undated).

have described previously (e.g., Riley, 2004; Berrick, 2007). For example, the "open" nature of rail systems, encompassing multiple access points and hubs serving multiple carriers on which passengers freely move about, makes them vulnerable to attack. Consider that there are more than 3,400 rail stations and nearly 33,000 miles of track in the United States (APTA, 2006).[3] Also, passenger volume and density make rail systems vulnerable by concentrating large numbers of people in confined spaces. On an average weekday, passengers make more than 12 million unlinked trips by rail, not counting those made on Amtrak (APTA, 2006).[4] For some rail systems, their "iconic" status and relation to the regional economy and daily life may increase their vulnerability. More generally, they present an opportunity to disrupt a distributed network by a single attack. For terrorist organizations seeking to produce mass-casualty attacks, such a "target-rich environment" makes rail systems particularly attractive.

The physical features and environments of rail systems also make them difficult to secure. Rail systems vary in age, design, and usage of above- and below-ground infrastructure. This often makes retrofitting rail systems to include new security technology, which is difficult and costly. For example, retractable bollards may be a desirable measure to implement at rail power-plant entrance and exit access points. However, even though the cost to procure bollards is relatively low, installing them can be expensive, if not impossible, depending on the composition of the ground infrastructure immediately below their desired placement. If the operation of bollards is not properly coordinated with security, they can also diminish emergency access when the situation arises, which highlights the need to consider carefully the potential trade-off between each security-improvement benefit while maintaining the more desirable, operational features of rail systems, such as easy access, privacy, efficiency, and ease of use.[5]

Finally, the U.S. government and railway operators have made attempts to improve railway security. Transportation Security Administration inspectors and rail operators have conducted security-risk readiness assessments (Hawley, 2007); also, various security measures have been considered and implemented, such as greater surveillance, public-awareness campaigns, and general response planning.[6] Yet there is still much to be done, according to the findings in a recent GAO report focused on the ability of the U.S. Department of Homeland Security (DHS) to objectively assess the risks of terrorist attacks, the vulnerability needs of critical infrastructure assets, and the equitable

---

[3] This includes commuter, heavy, and light rail systems, including Amtrak.

[4] *Unlinked passenger trips* refers to the number of passengers who board rail vehicles. They are counted each time they board a vehicle regardless of the number of vehicles they use to travel from their origin to their destination. See APTA (2006).

[5] For a discussion of the economic consequences of such trade-offs, see Jackson, Dixon, and Greenfield (2007).

[6] The Federal Transit Administration (FTA) compiled a list for assisting passengers and rail operators to observe of suspicious indicators of questionable activity and unattended packages and the recommended course of action to take in these situations as part of its Transit Watch program. See FTA (undated).

allocation of grant funding across urban areas for improving rail-passenger security (Berrick, 2007). For example, at the operational level, not all rail workers appear to understand their roles and responsibilities in improving passenger security. Surveys of rail workers suggest that rail engineers and track workers have little information about the security framework and how to respond during a terrorist event (Teamsters Rail Conference, 2005). This could potentially undermine any effort that attempts to promote their vigilance in identifying and acting on threats.

Objectives and Scope

The goal of the study on which this book reports was to develop a framework for security planners and policymakers that can be used to guide security planning and operational decisions—a framework that is driven by assessments of the foremost threats to, and vulnerabilities of, passenger-rail systems and of the cost-effectiveness of mitigation strategies for addressing those threats and vulnerabilities.

The study focused on passenger, as opposed to freight, rail systems. Unless otherwise noted, the terms *passenger rail* and *rail* refer to heavy-rail systems, defined as electric railways (including metro, subway, rapid-transit, or rapid-rail systems) capable of handling heavy volumes of traffic. Heavy rail is characterized by high speed and rapid-acceleration passenger cars operating singly or in multicar trains on fixed rails. They also operate on separate rights of way from which all other vehicular and foot traffic is excluded. Moreover, they are generally high-platform loading. Within the United States, examples of heavy-rail systems include the Metrorail in Washington, D.C.; Metropolitan Atlanta Rapid Transit Authority (MARTA); the Metro Red Line in Los Angeles; and Bay Area Rapid Transit (BART) in San Francisco and Oakland (APTA, undated[d]). Our analysis centers on heavy-rail systems, and, although it may offer some parallel lessons for them, it does not specifically address light- or commuter-rail systems.[7]

Because of the tremendous variation in the types of rail systems, and because we do not wish to publicly display the operational and security features of any specific rail system, the assessments of risk and the cost-effectiveness of mitigation strategies are based on a notional rail system. Our notional rail system is not real, but it has the typical features of rail systems found throughout the United States, including those

[7] By contrast, light-rail systems are composed of lightweight passenger cars operating singly or in short, two-car trains on fixed rails. Light-rail cars are generally electrically powered, run on exclusive right-of-way tracks, and are not separated from vehicular or pedestrian traffic over the majority of their distance. These are commonly called *streetcars*, *tramways*, or *trolleys*. Commuter-rail systems are electric or diesel-propelled railways operating between a central city and its adjacent suburbs. Commuter-rail service, also called ***metropolitan rail***, ***regional rail***, or ***suburban rail***, is characterized by multitrip tickets, specific station-to-station fares, and the presence of only one or two stations in the urban area's central business district. See APTA (undated[b]).

that we studied in depth. More detail on the rail systems we visited and the interviews conducted is highlighted in the subsequent chapters.

Approach

A primary goal of rail-security policy is to determine the most cost-effective strategies for mitigating the risk of rail passengers to terrorist incidents. As described more fully in Chapter Three, risk is a function of threat (presence of terrorists with intent, weapons, and capability to attack), vulnerability (likelihood of damage at a target, given an attack), and consequences (nature and scale of damage if the attack succeeds). This book focuses mostly on reducing risk by reducing vulnerabilities and limiting consequences. Reducing risk by acting against threat is the responsibility of policymakers elsewhere (see Willis et al., 2005).

We seek to meet this goal by adapting an analytic framework that RAND researchers developed and employed on other security-resource allocation problems (e.g., Stevens, Schell, et al., 2004; LaTourrette et al., 2006). The present application is novel in that it represents the first use of cost-effectiveness assessment methods in improving passenger rail–system security. In addition, the rail environment is considerably more complex than the other applications of the framework, in particular given passenger rail's function of moving large numbers of people quickly and relatively inexpensively.

Conceptually, the steps in using the framework to make security-resource allocation decisions are relatively simple. First, the framework is used to empirically assess the risk to rail systems from terrorism. This analysis generates, in turn, a list of security-improvement options (SIOs) that addresses the scenarios (based on target location and attack modes) assessed as high risk. The options are then assessed as to their relative cost-effectiveness. Throughout, the framework offers conceptual ways of thinking about security provisions, raises critical questions that must be answered about the trade-offs implicit in security investments, and highlights how analysis can inform security planning. Detailed discussion about specific aspects of the framework is presented in subsequent chapters.

The analyses that emerge from using the framework are general enough to allow the work to be made publicly available but specific enough to provide guidance from the national level all the way down to individual rail systems. These qualities, combined with the book's synthesis of issues related to both rail-system vulnerabilities and how to cost-effectively reduce them, contribute to its broad applicability and utility for security planners, policymakers, and researchers.

Outline of Book

The next chapter assesses the key attack threats confronting rail transportation and the consequences of attacks, while Chapter Three enumerates the vulnerabilities of and assesses the risk to a typical, but notional, rail system from the key threats. Chapter Four describes the notional rail system and baseline set of operational security measures in place for protecting passengers. Chapter Five outlines the assessment framework and compares the effectiveness and costs of SIOs and strategies to address high-risk attack scenarios against the notional rail system. The final chapter discusses key policy lessons learned for improving rail security based on the overall analysis. Appendix A contains the full, sequential, qualitative risk analysis we conducted, which underlies the findings we discuss in Chapter Three. Appendix B contains the basis of the cost estimates of SIOs, lethal characteristics of different attack modes, and the performance of the options at preventing or mitigating the damage consequences of terrorist attacks, all of which are the back-up details relevant to performing the cost-effectiveness analysis discussed in Chapter Five.

CHAPTER TWO

What Are the Key Rail-Attack Threats and Their Consequences?

Introduction

As illustrated by the examples provided in the previous chapter, passenger-rail systems have been attractive targets for terrorist attacks through much of the history of modern terrorism. Open and accessible by design and necessity, crowded with people, and key for the functioning of economic and daily life in the cities they serve, these systems represent both attractive and high-impact targets. Their openness and high usage also make them difficult to secure. As the attacks in Madrid and London demonstrate, attacks on rail systems can result in high casualty counts.

In this chapter, we discuss the key rail-attack threats and the consequences of attack. To assess the risks of terrorists targeting passenger railways, we examined available data on past terrorist attacks on such systems. The majority of the data came from the RAND-MIPT Terrorism Incident Database (National Memorial Institute for the Prevention of Terrorism and RAND Corporation, ongoing),[1] although the research team supplemented those data with descriptions of incidents from previously published examinations of terrorism against rail targets and from incidents included in other databases (Jenkins, 1997; Jenkins and Gersten, 2001; Rabkin et al., 2004; Monterey Institute of International Studies, undated[a]). Examining the data from these sources provided a picture of rail attacks over a long period of time; we looked at attacks that occurred from the 1920s up to the end of 2006. For this examination, the more inclusive definition of *rail targets* was used rather than limiting the assessment to attacks on only passenger-rail targets.[2]

Because of major differences across the data sources, the majority of incidents are very recent (e.g., 40 percent of the 886 attacks for which information is available

[1] The RAND-MIPT Terrorism Incident Database is a comprehensive databank of global terrorists and incidents. See National Memorial Institute for the Prevention of Terrorism and RAND Corporation (ongoing).

[2] In our data set, approximately 55 percent of the attacks could be identified as attacks on passenger-rail targets, but only 10 percent of attacks could be positively identified as having been staged on freight-rail targets. The remaining 35 percent could not be categorized either way. Given the comparatively small number of definitively freight incidents and the likelihood that eliminating those incidents would not, in fact, remove all freight-related incidents from the data set, we opted to work with the data set in its entirety.

occurred between 1990 and 2000, and 41 percent between 2000 and 2006.) Given that the interest of this work is focused on security measures that can be taken now against today's (and tomorrow's) terrorist threat, this bias toward recent events is not necessarily a problem. The recent past provides at least a baseline from which to consider adversary behavior and to explore how it will either remain the same or diverge from established patterns.

This recent-past bias means that the data we describe do not provide a representative picture of terrorist activity against rail targets over this full time period. As a result, we will cautiously use the information drawn from this examination of past events to make *descriptive* points about the types of attacks groups have staged, the targets they have attacked, and their outcomes, rather than quantitative arguments about absolute levels of risk for particular attack types or scenarios. In addition, it is broadly accepted that there have been changes in the nature of the terrorist threat in recent years, specifically that there are more terrorist groups seeking to carry out mass-casualty attacks. A number of recent terrorist operations have sought to do this through the use of many simultaneous bombings and the pursuit—though fortunately not the use—of unconventional weapons. Given that the role of security efforts is to prevent future attacks, the potential effects of such changes must be considered in planning.

In the context of the wider terrorist threat, attacks on rail systems represent only a small fraction of overall terrorist activity. For the years 1998 through 2006, the RAND-MIPT Terrorism Incident Database contains approximately 24,000 attacks. Our data set on rail attacks, drawn from that database and others, includes only 455 rail attacks during those years, meaning that attacks on rail targets constitute less than 2 percent of overall recent terrorist activity. Looking at the fraction of attacks on rail targets over time, there is also no indication that terrorists are increasingly targeting these systems, although there is some evidence that they are shifting more generally to softer targets (Libicki, Chalk, and Sisson, 2007; Chalk et al., 2005). Nevertheless, prominent, recent operations against rail targets by groups either affiliated with or sympathetic to al Qaeda are a cause for concern, particularly since those attacks have resulted in considerable numbers of causalities and significant damage to the targeted systems.

What follows is a discussion of the weapons and tactics used against rail systems, the targets of rail attacks, and the outcomes of such attacks.

Weapons and Tactics Used Against Rail Systems

Table 2.1 shows that, consistent with data on terrorists' tactical choices in general, the majority of the terrorist incidents that occurred on rail systems involved bombings. Such operations represented 80 percent of the attacks for which information was

Table 2.1
Terrorist Tactics in Rail Incidents

Tactic	Number	Percentage
Armed attack	55	6
Arson	29	3
Barricade or hostage	2	0
Bombing	708	80
Hijacking	2	0
Kidnapping	3	0
Sabotage	49	6
Unconventional attack	24	3
Unknown	9	1
Logistics activity (nonattack)	5	1
Total	886	100

SOURCES: Analysis of rail-incident data compiled from National Memorial Institute for the Prevention of Terrorism and RAND Corporation (ongoing), Jenkins (1997, 2001), Rabkin et al. (2004), and Monterey Institute of International Studies (undated[b]).

NOTE: *Sabotage* refers to the damaging of rail systems without the use of a weapon (e.g., removal of rails, manual damaging of equipment). *Logistics activity* refers to incidents in which terrorist activity occurred on a train but was not part of an attack operation. For example, if a terrorist group were moving a bomb from one place to another and it detonated inadvertently, such an incident would be included in this category. Bombs found in rail vehicles or stations that were not yet set to detonate are also included here.

available, with the next most common operations being armed attacks and sabotage (which each represented just 6 percent of the total incidents).

Not unexpectedly, given the dominance of bombing operations, more than three-quarters of the attacks used explosives (Table 2.2).[3] However, illustrating that terrorist groups do indeed seek to cause disruption in rail systems, sometimes without even staging an actual attack, 8 percent of the incidents on which data are available were hoaxes or threats that did not involve an actual weapon.[4]

[3] The fraction of bombing incidents and the fraction of incidents using explosives are not equal because bombing incidents can be staged with incendiary weapons and because bomb threats are included in the bombing category in the RAND database.

[4] This figure is likely an underestimate because of how most data sets on terrorism, including the RAND-MIPT database, are assembled. Terrorist incidents are identified in media reports and databases. The nature of threats and hoaxes, even those carried out by recognized terrorist organizations, is such that they may be less likely to be reported in the media than are actual operations and could, therefore, be underrepresented in available data sources.

Table 2.2
Weapons Used in Rail Incidents

Weapon	Number	Percentage
Explosives	643	77
Fire or firebomb	39	5
Firearms	51	6
Chemical agent	17	2
Radiological agent	3	0
Threat	65	8
Unknown	18	2
None	1	0
Total	837[a]	100

SOURCES: Analysis of rail incident data compiled from National Memorial Institute for the Prevention of Terrorism and RAND Corporation (ongoing), Jenkins (1997, 2001), Rabkin et al. (2004), and Monterey Institute of International Studies (undated[b]).

[a] This total reflects that sabotage incidents were not assigned a weapon type. There were 49 sabotage incidents (see Table 2.1), and 886 – 49 = 837.

The Targets of Terrorist Attacks in Rail Systems

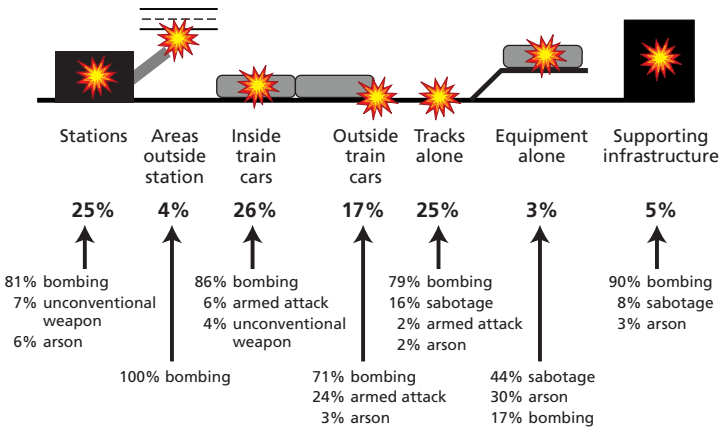
To assess how attacks have been distributed within these systems, descriptive information on each incident was reviewed and, where possible, the specific target of attack within the rail system was determined. Incidents were categorized as being targeted at one or more of the following: rail stations, areas outside rail stations, trains and their passengers from inside the train, trains and their passengers from outside the train, rail tracks, rail equipment, or supporting infrastructure.

In many cases, assigning targets was straightforward; for example, bombs placed inside rail cars fell clearly into a single category. However, in others incidents, attacks could have multiple targets, such as a bombing targeting a rail bridge, which was categorized as targeting both the tracks and the supporting infrastructure. In addition, some incidents did not fall cleanly into one category; for example, while an armed attack on a passing train was clearly targeted only at the train and its passengers, a bombing as a train passed or track sabotage could be aimed at damaging both the train (and injuring its occupants) and the tracks. In these cases, we made a judgment call based on available data; if a bombing clearly occurred as a train was passing, then the train was assumed to be the primary target, but, if it occurred when a train was not passing, we assumed that the bomber was targeting the tracks. Similarly, sabotage of tracks was assigned as targeting only the tracks themselves, even though, in many

cases, the intent of the sabotage was, likely, to derail later trains. Absolutely certain targeting assignments could be made only if information were available on the actual intent of the terrorists involved in the attacks. Such information is not available in most cases. As a result, independent assignment by separate analysts could produce somewhat different outcomes. Given the relatively broad categorization we performed of these data, we believe that the effect of such changes would be limited and would have the most effect for the most difficult assignments (e.g., the decision whether a particular track bombing or sabotage operation was actually targeting a train from outside).

Not enough information was available to categorize all incidents: Of the 886 incidents in the data set (and shown in the earlier tables), only 769 were assigned at least one identified target. Only a small subset of these (36 incidents) had multiple targets associated with them. Figure 2.1 summarizes the locations of attacks for which a target was identified, using the categorization of target locations given above. As the figure shows, three-fourths of the attacks on which data are available were approximately evenly divided among rail stations, inside train cars, or targeting the tracks of the rail system.

Figure 2.1
Locations of and Tactics Used for Rail Attacks



SOURCES: Analysis of rail incident data compiled from National Memorial Institute for the Prevention of Terrorism and RAND Corporation (ongoing), Jenkins (1997, 2001), Rabkin et al. (2004), and Monterey Institute of International Studies (undated[b]).
NOTE: Reported values are the percentage of all attacks that could be categorized by site targeted within the attacked rail systems. Percentages do not add to 100 because of rounding and the targeting of multiple sites by a single attack. Of 769 categorized attacks, 36 incidents (5 percent) had more than a single target associated with them. Percentages of tactics describe the distribution of attacks at each point in the system, reporting only the top three (or four, given a tie) tactics used. Tactical percentages may not sum to 100 percent because of rounding and omission of rarely used tactics.
RAND *MG705-2.1*

Given the practical differences among targets, the mix of tactics used to attack different parts of rail systems differed considerably. The vast majority of attacks at all points of the rail system were bombings, except for attacks on equipment alone, in which sabotage dominated. Armed attacks were most prominent in operations against trains (either from inside or outside). Not unexpectedly, given the practical requirements for using such weapons, unconventional-weapon usage (which included only chemical and radiological agents in this data set) was prominent in stations and inside train cars.

Outcomes of Past Terrorist Attacks on Rail Systems

A full understanding of the threat of terrorism to rail systems must have as its basis information not just on types and locations of attacks but also on the consequences of attacks when they occur. Such an understanding should be based not just on the casualties produced by attacks but also on the physical damage caused and the incident's effect on rail-system functioning.

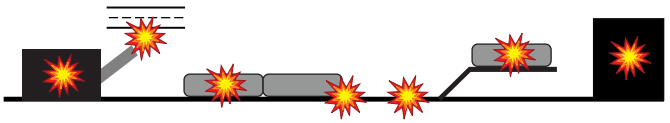
The effects of incidents on rail systems can vary considerably. An attack that damages a single rail car may have minimal effects if that car can be moved out of the way and postattack recovery and investigation can be carried out in a way that does not interfere with the system. In contrast, a large operation that damages key infrastructures (e.g., elevated track or bridges, control systems) could render a system inoperable until the damaged sections can be rebuilt. Furthermore, an attack's effects on ridership on a system—whether patrons will return quickly to daily use or are frightened into using other forms of transportation for extended periods—will also likely vary among attack scenarios.

Although some information about how attacks affected the rail systems themselves is available—e.g., the number of rail cars damaged in a bombing or the number of hours or days a line was shut down as a result of sabotage—not enough data are available to support a systematic assessment of the consequences of terrorist attacks.

However, data are generally collected on the injuries and fatalities resulting from most attacks. Across all terrorist attacks on rail systems that can produce casualties,[5] the average numbers of fatalities and injuries produced were four and 20, respectively (as shown on the far left of Figure 2.2). However, the injury totals must be interpreted with some caution, because they are driven largely by a single incident—Aum Shinrikyo's March 1995 attack on the Tokyo subway system using the chemical agent sarin.

[5] Attacks that "did not occur"—e.g., incidents in which security forces found and disarmed a device or disrupted a terrorist attempt to plant a bomb—are also excluded, as are hoaxes. Including both these types of events would increase the overall number of incidents across which these averages are being calculated and produce lower per-incident values.

Figure 2.2
Average Fatalities and Injuries Resulting from Attacks on Rail Systems, Overall and by Location of Attack



	Attacks overall	Stations	Areas outside station	Inside train cars	Outside train cars	Tracks alone	Equipment alone	Supporting infrastructure
Average fatalities	4	3	1	8	5	1	4	1
Average injuries	20 (13)	11	7	60 (30)	12	5	2	4

SOURCES: Analysis of rail incident data compiled from National Memorial Institute for the Prevention of Terrorism and RAND Corporation (ongoing), Jenkins (1997, 2001), Rabkin et al. (2004), and Monterey Institute of International Studies (undated[b]).
NOTE: Averages calculated across all attacks in which the potential existed for casualties to occur (e.g., excluding threats and attacks disrupted before initiation). Of 886 total incidents examined, 689 were included in calculation of these averages. Values were rounded to the nearest casualty. Numbers reported in parentheses in the figure for all attacks and attacks inside train cars are calculations excluding the Aum Shinrikyo attack on the Tokyo subway in March 1995, which produced a reported 5,000 injuries.
RAND *MG705-2.2*

In our data set, the number of injuries produced in that single attack is reported at 5,000.

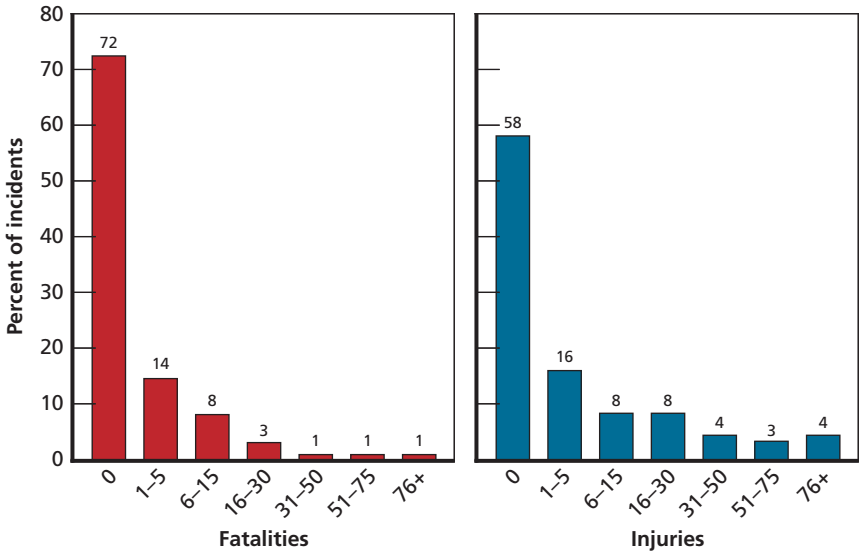
Estimates of the number of injuries produced in Aum's sarin attack vary widely. For example, Murakami (2001) could identify only 700 people by name who were injured in the attack. Fred Sidell (1996, pp. 2-32–2-33), a U.S. government physician who traveled to Japan in the days after the incident to learn about the response, reported that, of "5,510 casualties; they had a total of 12 deaths, . . . 17 critical patients; 37 severe, and 984 moderate. This leaves about 4,000 casualties who reported to medical facilities who seemingly had nothing wrong with them." Although the uncertainty around this particular value is wide, the reality is that there is unavoidable uncertainty associated with all casualty figures in terrorist attacks because of the processes through which the information is collected for inclusion. Without a clearer rationale for selecting a value different from that already included in our database for this particular incident and no others, we have calculated average injury numbers both with and without that value to show its effect on the overall estimated casualty figures. This bounds the effect of this incident, placing the actual value somewhere between the two numbers

we report here. With that incident removed, the average injuries per attack on a rail target drops to 13 (values in parentheses in Figure 2.2).[6]

While the influence of that specific attack is strong, the average fatalities and injuries in attacks on rail systems are driven largely by the results of disproportionately large attacks. In fact, the vast majority of attacks on rail systems (Figure 2.3) produced no fatalities (72 percent of incidents) or injuries (58 percent of incidents). The influence of such large incidents on aggregate measures can be reduced by examining the median number of fatalities and injuries in the data set. The median injuries and fatalities for attacks on rail targets producing at least one casualty are one fatality and 10 injuries.[7] This compares to median casualties across all terrorism incidents producing at least one casualty of one fatality and three injuries.

Looking at the results of attacks at different targeted locations, attacks on train cars (particularly from inside but from outside as well) produce greater-than-average fatality counts. Only attacks inside train cars result in a larger-than-average number of injuries, although attacks in stations and on train cars from outside also have comparatively high average injury counts. These observations are not surprising as attacks

Figure 2.3
Distributions of Fatalities and Injuries in Attacks on Rail Systems



RAND *MG705-2.3*

[6] This compares to average fatalities and injuries for all terrorist attacks in the RAND-MIPT Terrorism Incident Database of approximately 1.5 fatalities and 3.4 injuries per attack.

[7] If the large number of incidents producing no injuries or fatalities is included, the median for both is zero, both for rail attacks (reflected in the histograms in Figure 2.3) and for terrorist incidents overall.

on rail cars and stations are focused largely on targeting individuals, while attacks on other sites may be more focused on producing disruption or damage to the system itself.

Breaking down the results of attacks on rail systems by tactic (Table 2.3), sabotage incidents stand out for producing high fatalities and injuries, largely because of their potential for involving an entire train and, as a result, a larger number of potential victims. Armed attacks produce particularly high numbers of fatalities per incident, although the drivers of the elevated average are a small number of military-style attacks by large units that are, on the whole, irrelevant for the U.S. domestic security environment.

With respect to bombings, the most common mode of attack on rail systems, there is an important caveat in interpreting the average fatality data. Suicide-terrorism operations were relatively underrepresented in our data set (only six incidents were suicide operations, representing less than 1 percent of even the bombing operations). Suicide operations provide much more control over targeting and detonation and may contribute to the ability to evade certain types of protective measures. In an analysis of terrorist operations in general, Hoffman (2003) determined that suicide attacks are, on average, four times more lethal than average terrorist operations. As a result, larger representation of suicide operations—an attack mode that is unfortunately becoming increasingly common in the activities of modern terrorist organizations—could significantly increase the average casualties caused by bombing operations.

Table 2.3
Injuries and Fatalities in Rail Incidents, by Terrorist Tactic

Tactic	Average Fatalities	Average Injuries
Armed attack	8	13
Arson	0	0
Barricade or hostage	2	1
Bombing	3	13
Hijacking	0	0
Kidnapping	5	0
Sabotage	13	30
Unconventional attack	1 (0)	397 (13)
Overall averages	4	20 (13)

NOTE: Values in parentheses are averages excluding the Aum Shinrikyo attack on the Tokyo subway in March 1995, which produced a reported 5,000 injuries.

Lessons from the Threat Assessment

For assessing the current terrorist threat to rail systems and the cost-effectiveness of measures that could be implemented in response to that threat, the historical data describing attacks on rail systems have a variety of applicable lessons:

- Most of the threat to rail systems comes from bombings, although a variety of other tactics—including both chemical and radiological weapons—have been used against rail targets less frequently. *Thus, security measures must deal effectively with the threat of explosive devices but also must appropriately hedge against the potential for rarer attack modes (e.g., sabotage occurs much less frequently than bombings, but sabotage is much more lethal in terms of average fatalities and injuries per incident).*
- Most terrorist incidents in rail systems produce very few, if any, fatalities or injuries, and average fatalities in these incidents are driven by a comparatively small number of very damaging attacks. *As a result, even if security measures prevent only the largest-scale attacks, they could significantly reduce the human costs associated with this threat.*[8] Given recent large-scale attacks on rail systems in Madrid, London, and Mumbai, coupled with the desire of contemporary terrorist groups, such as al Qaeda, to produce mass-casualty events, the importance of preventing these macroterrorist events takes on added magnitude.
- Not unexpectedly, since terrorists target areas where passenger population is concentrated, *attacks inside train cars, targeting train cars from outside, and in densely populated stations are of particular concern*, based on the fatalities and injuries they produce.

There is an important caveat to this discussion of the terrorist threat to rail systems. Although historical data and the patterns of behavior they document provide a foundation for security decisionmaking today, more information is required in assessing the current terrorist threat. While recent behavior does provide a guide to what terrorists have done previously, assuming that the future will simply repeat those patterns could mean that novel tactics or attacks that have not yet come to pass will not be appropriately considered. An example of this is the relative underrepresentation of suicide operations in the historical data set of attacks on rail targets compared to the prominence of that tactic in contemporary terrorism. While it is neither practical nor desirable to base security planning on every possible terrorist scenario without considering how likely or unlikely each might be, prudence requires considering ways in which future behavior may reasonably deviate from the past.

[8] The average fatalities and injuries for all events (four and 20 [13], respectively) drops to three and eight if all events killing or injuring more than 100 people are eliminated. If all events killing or injuring more than 50 individuals are eliminated, the averages drop further, to two and five, respectively.

CHAPTER THREE

Qualitative Risk Assessment for a Notional Passenger-Rail System

Introduction

In the previous chapter, we described the threat to rail-transportation systems and the consequences of attacks. We now turn our attention to describing the vulnerability of passenger-rail networks to the threats previously described. To do so, we introduce two new elements to our analysis. The first is initial specification of a notional rail system. We use a notional system, rather than an actual system, to illustrate the complexity of rail operations while avoiding providing any confidential details about specific rail systems in operation in the United States.

Second, we specify attack scenarios. By specifying attack scenarios, we begin to assess the specific ways in which terrorists might attack rail systems and the resultant consequences; this, in turn, provides the foundation for understanding the risk that rail systems face. The sources for the attack scenarios were largely the same as for the threat assessment. Sources included official documents from government and industry organizations (e.g., incident reports, security assessments, policies, manuals), analytical and evaluative reports from research and government organizations, media accounts of passenger-rail attacks, and databases such as the RAND-MIPT Terrorism Incident Database (National Memorial Institute for the Prevention of Terrorism and RAND Corporation, ongoing). Thus, what follows in the remainder of this chapter is a discussion of the notional rail system we use in considering vulnerabilities, the attack scenarios we lay out, and an assessment of how vulnerable the notional system is to the various attack scenarios.

Laying Out a Notional Rail System

In the previous chapter, in which we discussed threat, we laid out a schematic of a rail system to illustrate where attacks have historically occurred. However, contemporary rail systems, particularly subway and commuter systems within major cities, present a more varied potential-target environment than did the schematic we showed earlier. In trying to determine attack scenarios, highlighting the vulnerabilities of rail systems to

such attacks, and considering mitigation strategies to address such vulnerabilities, we need a more detailed model of the rail system.

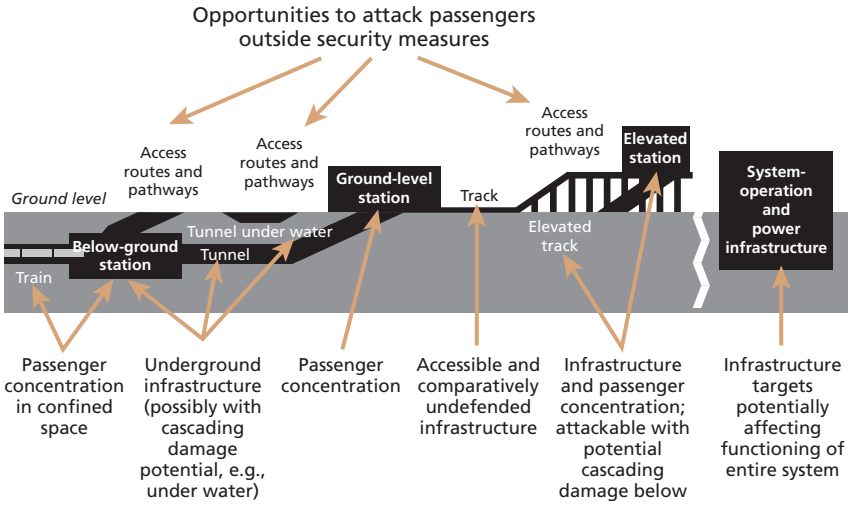
Figure 3.1 shows a somewhat more detailed model of such systems, capturing more of the variety in potential points of attack. The model is not intended to correspond to the particular characteristics of any individual subway or passenger-rail line but rather to capture the main elements of above-, below-, and ground-level passenger-rail–station transportation systems.

Consistent with the general taxonomy shown in the figures in Chapter Two, locations within the system are identified based on the opportunity they provide for potential attack either on the passengers in the rail system (e.g., passenger concentration in stations or trains) or on the system itself (attacks on rails or subterranean infrastructure).

Determining Attack Scenarios

Addressing the risk of terrorism in rail systems requires putting measures in place that address the variety of ways in which an adversary could attack each of the elements of the system shown in Figure 3.1. The ways in which terrorist groups have attacked these systems in the past (as detailed in Chapter Two), coupled with a broader understanding of the ways in which such groups could potentially attack different system components, make it possible to define a set of attack scenarios (where an *attack scenario* is

Figure 3.1
The Rail System as a Terrorist Target: A Notional System



RAND *MG705-3.1*

defined as the use of a specific attack mode at a given target) that can be used to assess the effectiveness of different mitigation and security strategies. Such an effort seeks to capture not just the ways in which groups have used particular weapons in the past but also ways in which they might use them in the future. For example, although our data set does not include the use of large-scale incendiary weapons to harm rail passengers, terrorists have used such weapons in other contexts.

The importance of this broader assessment is demonstrated by the fact that terrorist groups can apply tactics and techniques developed in other contexts to attacks on rail systems. For example, recent experimentation by groups in Iraq with the use of chlorine in improvised chemical weapons is a troubling development from the perspective of rail-security planning even if such weapons have only been used in a very limited way against rail systems in the past.

For our assessment of vulnerabilities in this chapter and of security measures in the following chapter, we consider the following attack types:

- *Explosive devices.* The prevalence of explosive devices in past terrorist operations suggests that such attack modes will feature prominently in future threats to these systems. Timed explosive devices can provide a way for a terrorist organization to stage attacks while preserving its human capital; suicide operations using similar technologies and components provide an alternative strategy for groups to increase the potential effectiveness of such attacks at the cost of their group members. In looking at explosive devices, we have simplified our examination to consider two broad classes of devices: large (e.g., vehicle-size bombs) and small (e.g., portable explosives that can be brought into a rail system). Terrorists could design operations around single devices targeting one element in a rail system or, by using multiple devices, increase the scope of an attack. For large explosives, we specifically use the term *vehicle bombs* to facilitate narrowing down the set of relevant SIOs discussed in Chapter Five and for characterizing the potential consequences by drawing on comparable assessments of this type of terrorist attack from previous RAND research (Stevens, Schell, et al., 2004).
- *Incendiaries.* Materials and devices to produce fires have been used in a number of past rail and other terrorist operations. We have simplified our examination to consider two classes of incendiaries: large (e.g., a vehicle carrying flammable cargo) and small (e.g., a Molotov cocktail). Incendiaries can be very basic or more sophisticated devices that can be triggered remotely or with a time delay.
- *Armed attack.* Use of standard firearms and other infantry weapons have been prominent in past terrorist and criminal action on and against subway and rail systems. Such weapons could be used in operations ranging from small-scale attacks (e.g., individual shootings to inspire fear) to higher-impact assaults (e.g., multiple-shooter attacks on crowded train cars).

- *Unconventional weapons.* While the actual level of threat from the terrorist use of unconventional weapons is uncertain (see, for example, Jackson, Baker, et al., 2005; Hoffman, 1999), rail systems (particularly enclosed cars and underground areas) are potentially attractive targets for chemical, biological, and radiological attacks. The concentration of individuals within enclosed spaces could help to compensate for a terrorist group's limited sophistication in designing and deploying such weapons, thereby increasing the potential impact of their use.
- *Sabotage.* Groups across the terrorism spectrum have used sabotage, either to cause disruption or to produce accidents resulting in casualties. Such operations have the advantage of not requiring any weapons, although they do require some knowledge of system operations to increase the predictability of their outcomes.
- *Hoaxes or threats.* While hoaxes and threats do not directly produce any casualties[1]—and are, therefore, most desirable for groups interested in disruption in addition to destruction—they can be an element of a terrorist campaign. System reactions to threats will shape the level of impact that this tactic can have, and the credibility of such attacks will depend on whether they are being used within the context of an actual violent campaign (the hoaxes are "supported" by real attacks) or are being done in isolation.

Note that we have not included all the ways in which a terrorist organization could potentially deliver particular weapons to a rail system. For example, a mortar could be used to attack above-ground elements or trains when they are on the surface, a specific scenario that our simplified set of attack modes does not fully address. Such simplification is partly to limit the complexity of subsequent analysis, but it is also based on the fact that (as open and accessible sites) such delivery mechanisms are not needed at this time to deliver explosives to these targets. If such systems are hardened in the future, these adaptation pathways might need to be considered at a later date (see, for example, Jackson, Chalk, et al., 2007).

Qualitatively Assessing Terrorism Risk

To develop security strategies for protecting passenger-rail systems, it is necessary to move from descriptions of how terrorists have attacked in the past and the many different ways in which they might attack in the future to a more systematic discussion of the terrorism risk that these systems face. Terrorism risk can be viewed as a function of three components: threat, vulnerability, and consequences (Willis et al., 2005).

[1] Hoaxes and threats can produce casualties depending on individual and staff reactions to the event (e.g., people stampeding in a panicked response to a hoax). However, these reactions are difficult for adversaries to predict and produce with a high degree of certainty.

- The *threat* to a system is produced by the presence of terrorist groups that have both the intent and the means (the weapons and capability needed) to attack it. The attack modes that groups have used in the past and the ways in which they could be applied in the future define the threat component of the risk to these systems. Threat can be expressed as a probability that a system will face a particular type of attack at a specific target location in a given period. The prominence of bombing operations in past terrorist attacks on rail targets (shown in Table 2.1 in Chapter Two) suggests that systems face a much larger threat from bombs than from other attack modes.
- A system's *vulnerability* to particular attack modes determines the likelihood that damage will occur if it takes place at a specific target location. Vulnerability is determined by the nature of the system (e.g., hardening infrastructure and facilities) and the set of baseline security measures that are already in place to protect the security of passengers. This term can also be viewed as a probability—the chance that the attempted attack will produce local damage at a specific rail station or rail line rather than failing to penetrate or shutdown the entire system or being defeated by other means. This section and the next chapter expand on factors that affect vulnerability assessments across the rail system.
- *Consequences* refers to the nature of the damage that will occur if a staged attack succeeds. The consequences of terrorism can impact either rail passengers (as disruption or direct injury) or the functioning of the system (as damage or shutdown). Potential consequences can differ markedly among different types of attacks (shown in Table 2.3 in Chapter Two) or depending on the target of the attack within the rail system (shown in Figure 2.4 in Chapter Two).

The key analytical insight is that, from the perspective of security planning, it is risk—the combination of all three factors—that is the core concern. The presence of vulnerability is not necessarily a problem if no threat exists to exploit it or the consequences of someone doing so are minor, and even low-probability scenarios might merit security attention if the consequences (if they are realized) are sufficiently dire.

Although there is a wide variety of potential attack modes and targets within these systems, all parts of a rail system are not equally vulnerable to all attack modes. For example, practical access constraints mean that the use of very large explosive or incendiary devices in underground parts of these systems is very unlikely. Similarly, even if an attack can be staged with a given attack mode, some are likely to be more effective in some parts of a system than in others. For example, although a chemical attack could be staged in an elevated rail station open to the air, such an attack would be less effective than one staged in an underground station. Similarly, an unconventional weapon could be released in a tunnel in hopes that it would affect passengers in trains going through the area, but doing so would likely be inferior to releasing it inside the train cars themselves. As a result, even before the security planner begins arraying

available countermeasures against individual threats, an initial filter can be applied to highlight which attack modes are of most concern at which points in a rail system.

The results of this qualitative assessment of risk are summarized in Figure 3.2, in which attack scenarios are categorized into high, medium, and low risk based on sequential estimates of the threat (based on past terrorist use of the attack modes against specific rail target locations), vulnerability (based on the practical and operational constraints that shape the applicability and utility of an attack mode against specific parts of the rail system), and the potential consequences of each attack (based on the average fatalities resulting from past uses of specific weapons and of attacks at particular parts of rail systems and a qualitative assessment of economic consequences of different attack scenarios). Appendix A includes the full, sequential, qualitative risk analysis.

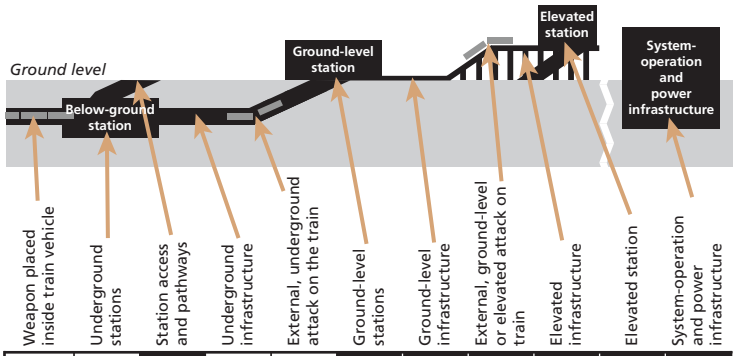
Figure 3.2 reproduces Figure 3.1, grouping the points in the system that provide the opportunity for attack (i.e., the targets) all along the top of the figure. Those points of attack are used as the columns in a table in which the eight attack modes described above are the rows. The intersection of the columns and rows yields a cell in the table for each attack scenario, which is coded into the three risk categories described above. Attack scenarios that appear particularly low risk because of significant practical constraints (e.g., use of a vehicle bomb underground) are left blank.

If we look at the cells in Figure 3.2, we can make some observations based on this simple, common-sense, qualitative filtering. First, some rail-attack modes are more of a concern than others. For example, the use of small explosives is a high or medium risk for most targets, while hoaxes or threats pose a risk for only a few targets (in this case, high risk for the system-operation and power-infrastructure target, likely producing disruption to the rail system rather than casualties, and low for other sites in the system).

Second, some rail-attack targets are more of a concern than others. For example, the target of system-operation and power infrastructure is a high or medium risk for seven of the eight attack scenarios. Then again, underground infrastructure is less of a target when assessed against the attack scenarios, with only one of the attack scenarios (sabotage) posing a high risk and small explosives posing a medium risk.

It is important not to read too much into the assessment. This type of qualitative culling of potential attack scenarios provides a first filter through which to view the appropriateness and value of security measures, which are discussed in the next two chapters. Measures will be of much less value if they are deployed to prevent attacks posing much lower risk because of the practical difficulties of carrying them out effectively.

Figure 3.2
Summary of Qualitative Terrorism-Risk Levels Associated with Different Terrorist Attack Scenarios



	Weapon placed inside train vehicle	Underground stations	Station access and pathways	Underground infrastructure	External, underground attack on the train	Ground-level stations	Ground-level infrastructure	External, ground-level or elevated attack on train	Elevated infrastructure	Elevated station	System-operation and power infrastructure
Large explosive			High			High	High	High	High	High	High
Small explosive	High	High	High	Medium	High	High	Low	High	Medium	High	High
Large incendiary			Medium			High	Low	High	Low	Medium	Medium
Small incendiary	High	High	Low		Low	Medium		Low		Medium	Medium
Armed attack	High	High	High		Medium	High		High		High	Medium
Unconventional weapon	High	High	Medium			Medium				Medium	Low
Sabotage	Medium			High	High		High	High	High		High
Hoax or threat	Low	Low	Low			Low				Low	Medium

NOTE: Although Figure 3.1 includes the particular risk of attacks on underground infrastructure that is below water, the risk analysis reported here includes only generic underground infrastructure and does not consider the risk added when that infrastructure is below water. This is because the rail system that served as the basis of the cost-effectiveness analysis reported in subsequent chapters did not include underground, underwater segments.

RAND *MG705-3.2*

CHAPTER FOUR

Baseline Security and Operational Characteristics of the Notional Rail System

Introduction

Ultimately, we want to identify security measures that will reduce terrorism risk to rail systems in the kinds of attack scenarios detailed in Chapter Three. Before we analyze the effectiveness of SIOs, we must both further describe our notional rail system and characterize security that it maintains. Thus, in this chapter, we provide a complete description of the notional rail system and define the baseline (or existing) set of security measures (and their performance) across the system. This collective set of information provides the groundwork for Chapter Five, in which we identify and assess the cost-effectiveness of different SIOs at providing incremental improvements to the baseline level of security.

In addition to the various sources described in Chapter Three, we interviewed rail personnel and visited several rail systems to provide background information and to identify the range of security measures currently in use in rail systems. We interviewed those directly responsible for administering and securing domestic and international passenger-rail systems. We conducted comprehensive reviews in Washington, D.C.; New York City; London; and Madrid by interviewing key respondents who represented rail operators, security departments, professional associations, unions, and various government offices related to transportation and policy. We also talked with respondents from various other U.S. rail systems and institutions.[1]

We chose to collect primary information in these cities for several reasons. First, these cities have varied forms of experience with rail attacks. The rail systems in London

[1] In all, we had discussions with representatives of the following organizations: American Association of Railroads (AAR), American Public Transit Association (APTA), British Transport Police (BTP), Metropolitan Police in London, London Underground, Los Angeles County Sheriff's Department, Metro de Madrid, Metropolitan Transportation Authority in New York City, New Jersey Transit, New York City Police Department (NYPD), Port Authority of New York and New Jersey, Port Authority Trans-Hudson Corporation (PATH), San Francisco Municipal Transportation Agency (SFMTA), Cuerpo Nacional de Policia (CNP, Spain's national police force), Red Nacional de Ferrocarriles Españoles (RENFE, Spain's national railway network), Administrador de Infraestructuras Ferroviarias (ADIF, Spain's railway-infrastructure administration), Department for Transport in the UK, Home Office in the UK, Network Rail in the UK, Transport Salaried Staffs' Association (TSSA, in the UK), DHS, and Washington Metropolitan Area Transit Authority (WMATA).

and Madrid have experienced actual attacks, the system in New York has thwarted several planned attacks, and there was an attack allegedly planned for the system in Washington ("London Attacks," 2007; "Madrid Train Attacks," 2007; Rashbaum, 2007; Associated Press, 2007; Lengel and Eggen, 2003). We therefore expected that the rail systems in these cities would offer lessons about risk and the effectiveness of different SIOs. Second, examining international systems allowed us to learn about innovative practices that may not be employed in the United States. Third, both New York and Washington have heavily used metropolitan rail systems. Yet, equally important, they have a heavily used intermetropolitan rail system connecting them (Amtrak). Selecting these cities allows us to simultaneously examine the rail system within and between two of the United States' most utilized—and perhaps most at risk—rail systems.

The notional rail system and the baseline set of security measures described in this chapter are based on a representative aggregation of common system attributes, cross-cutting security measures, and other relevant information collected and compiled from the rail-operation and security representatives noted.

Defining the Baseline Security Measures

In general terms, we defined the baseline set of security measures for the notional rail system as consisting of those most representative security features that are either already in place or scheduled for implementation (with firm budget commitments) across the majority of case-study rail systems we visited. We assumed that the notional rail system, located within a major metropolitan area, would have the following baseline security measures in place:

- *Perimeter surveillance system* comprised of two CCTV cameras located at each of the ground-level entrances and exits of all tunnels and underground passageways where the railroad tracks operate. The fiber-optic lines are in place to transmit video data feeds to monitors located within an operation-control center. Trained rail-operation staff are located at each of the monitors on a 24/7 basis. CCTV cameras are also located at ground-level railroad crossings.
- *Rail-station surveillance systems* comprised of CCTV cameras installed at the entrances and exits (e.g., pointed to outside street entrances, in passageways) and within the infrastructure, concourse areas, corridors, escalators, and the like leading to the train platforms. The surveillance system includes fiber-optic communication links to provide video data feeds to monitors located both within each of the station-operation security centers and back to one of several dedicated monitors within one operation-control center serving all the stations within the system. Trained rail-operation staff are located at each of the monitors on a 24/7 basis.

- *Uniformed patrols* consisting of assigned transit security police are deployed on a regular basis on duty 24/7 across each of the stations, with more available during peak hours and fewer on duty during off-peak hours. They are all equipped with handheld, portable radios that also include a GPS function for tracking their position and location. During peak hours, one or more of the transit-security police are deployed at all street-side station entrances, exits, and other external passageways.
- *Rapid-deployment forces* are also available and on call as needed, comprised of specially trained bomb squads and hazmat patrol teams.
- *Automated vehicle locator (AVL) system* located at the operation-control center for detecting unusual delays in trains within any one of the many lines within the notional rail system.

In addition to having a complete description of each of the rail system's baseline security measures—including the force levels, number of CCTV cameras and locations, and other measures that are currently in place—it is important to understand the breakdown of the total number and specific locations of each of the elevated, underground, and ground-level stations, as well as the hub-spoke network arrangement of the rail system's rail lines.

The type of station and location—whether rural, in an urban area within a highly populated business district, or adjacent to government buildings—should be considered and integrated into the overall tailoring, prioritization, and time-phasing of a preferred set of SIOs recommended as part of a security implementation plan. Assessing the vulnerability of individual stations within a rail system to help prioritize locations to implement SIOs is not without precedent.[2]

Notional Rail System Description

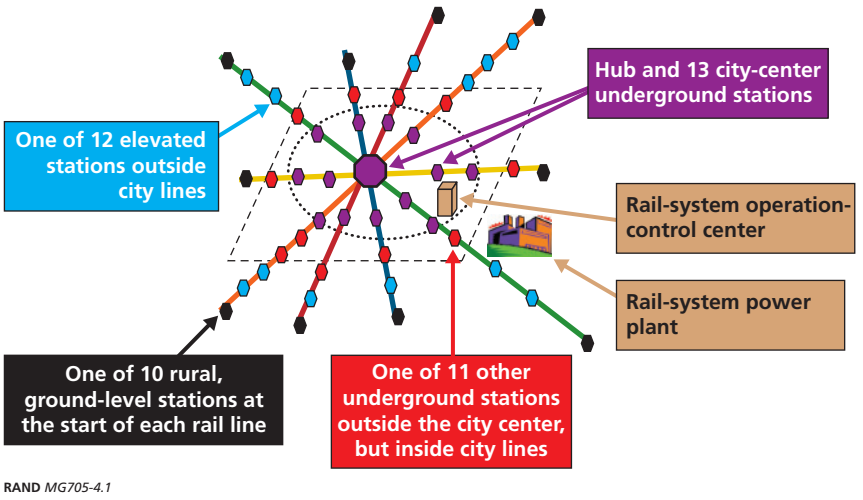
For our notional rail system, we assumed a relatively simple rail network consisting of five spokes of unique rail lines going directly into one hub, or central, station, with the only transfer point between these lines located at the hub station.[3] This is depicted in Figure 4.1.

---

[2] One passenger-rail site we visited has performed vulnerability assessments for each station in its system, and it has a policy in place to implement SIOs (e.g., by setting unique procedures, adding blast-resistant containers) as needed to mitigate terrorist threats specific to the station location. The vulnerability assessment also considered stations located in specific urban or regional areas adjacent to geographically sensitive locations (e.g., government buildings, stadiums).

[3] Even though some of the basic operational features of the notional rail system are representative of the case-study systems we visited, we elected not to make it overly complex and avoided identifying the specific features of any one system.

Figure 4.1
The Notional Passenger-Rail System Network



RAND *MG705-4.1*

There is a total of 47 rail stations (depicted as differently colored nodes in Figure 4.1). As displayed in Figure 4.1, the dotted, rectangular area around the rail system represents the city's municipal border, with the area outside this border being the surrounding suburban community. There are 22 rural stations, with 10 at ground level at the start of each rail line (displayed as black nodes) and 12 elevated stations (blue nodes) that are all outside the city limits. There are another 25 underground rail stations, including the main hub transfer station (large purple node), that are all within the city limits. There is also an oval line displayed in Figure 4.1 that further separates the 14 underground stations located within city center (purple nodes) from the 12 other underground stations outside the city center and within the municipal city limits (red nodes).

Through the 47-station system, we assumed that there is a total of 100 directional route miles, 120 track miles, and 360 passenger-carrying rail vehicles.[4] Since the track is routed above ground on bridges and below ground through tunnels leading to the 12 elevated rural and 25 underground stations, segments of the rail cover a directional route of a total of 30 miles that are at ground level for the rail vehicles to directly service the 10 ground-level stations, and another 30 directional route miles of rail go through tunnels through the 25 underground stations. As part of the cost-effectiveness assessment, all this information is relevant to estimating the investment cost and recur-

[4] The directional route and track miles and the number of rail vehicles were estimated based on computing ratios from comparably sized transit agencies from APTA (undated[a], undated[b], undated[d]). The difference between track miles and route miles is the additional length required for parallel tracks or additional tracks for rail vehicle turnaround at the end of each line.

ring annual expenses for implementing the majority of the SIOs and is the basis for the estimates discussed in Chapter Five and in the first section of Appendix B.

As far as the total rail-operation, security, maintenance, and support employee head counts, we assumed a 24/7, three-shift staffing requirement and a full-time equivalent total of 2,000 personnel.[5]

In addition, and as part of the total head count, the notional rail system has one operation-control center that, as previously mentioned, has an AVL train-control system set of staffed workstations; it has other rail-operation and security-dispatcher workstations, where operators are linked by voice, radio, and data communications using fiber-optic equipment and cables to station rail operations, line managers, and uniformed patrols on duty, and personnel located at a separate power-plant control-center facility.

During morning and afternoon rush hours, the peak passenger density and the choke point from a security perspective would likeliest occur at the one hub station also located within the city center. Since none of the stations is a multimodal transfer point for a commuter-rail line or adjacent to an airport, the vulnerability assessment and potential set of SIOs recommended could focus on security gaps from street-level hub-station entrances and exits to the train platforms' interior areas.

From a terrorists' perspective, the primary hub-station area would be a very attractive target, especially during the morning and evening rush-hour times of peak passenger densities. Also, the hub station is within close proximity to the city center, where the majority of the business and commerce activities within the metropolitan area takes place.

When we discuss the effectiveness-assessment metrics and the cost-effectiveness approach in Chapter Five, peak and off-peak passenger densities both on trains on specific lines and across the 47 stations within the notional rail system will be described in more detail and used as the basis for assessing the level of damage from a potential terrorist attack in terms of the magnitude of fatalities, the recovery time before operations are restored, and the loss of rail-operating revenues caused by the attack.

Defining Security Layers for the Notional Rail System

We defined the layers of the notional rail system as the same set of physical locations, described in Chapter Three and displayed again in Figure 4.2, that have been the focus of past and projected areas for terrorist attacks—elevated, ground-, and below-ground–level stations, as well as the platforms, trains, tracks, tunnels, bridges, and other components.

---

[5] The estimated total head count is based on counts of the number of full-time and part-time employees per shift of comparably sized, heavy-rail transit agencies from various open sources, which we then scaled to the total number of 47 stations for the notional baseline system.

Figure 4.2
Potential Terrorist-Attack Targets

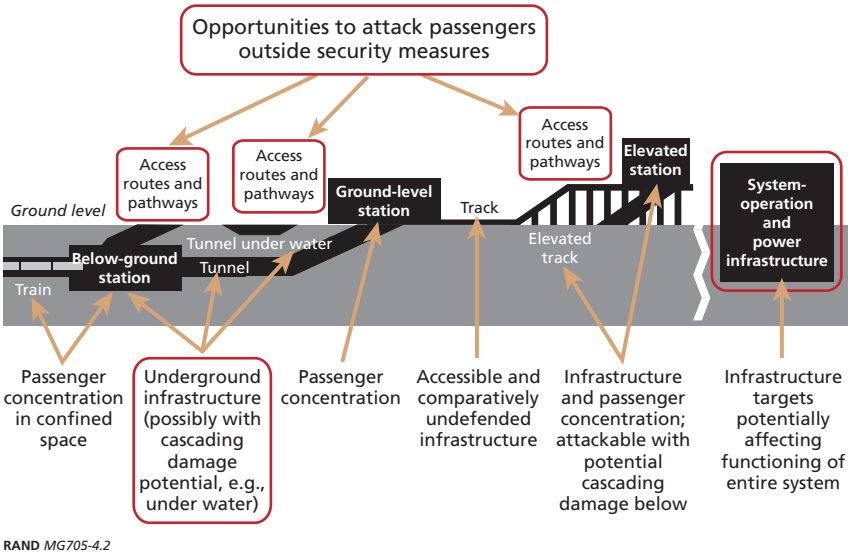


Table 4.1 provides a listing of all the potential target locations displayed in Figure 4.2 mapped across the five layers of our notional rail-security system's area of responsibility.

Figure 4.2 highlights (with red circles) the rail-system locations where *perimeter-layer* security measures would be warranted for protecting passengers' access routes and pathways leading to or exiting from these three types of rail stations: elevated, ground-level, and underground facilities and supporting infrastructure. Furthermore, other perimeter-layer locations (displayed in Figure 4.1 and Table 4.1) where security breaches by terrorists could take place include rail tunnels and entrances, bridges, and ground-level tracks where sections of a rail system's lines currently operate.

We also included two other potential terrorist-target locations as part of the perimeter layer: (1) the physical areas around and adjacent to the notional rail system's operation-control center and building infrastructure where the center is located[6] and (2) the area around the outside and adjacent to the notional rail system's central power-generation plant.

We realize that the safeguarding of the perimeter locations may be beyond the rail security force's jurisdiction and responsibilities. However, we included these perimeter locations in our notional system and the assessment process because we also recognized that, in today's resource-limited environment, multiple government, public, and private stakeholders have varying levels of vested interests. As confirmed by our

[6] As we learned from our case review of rail systems, operation-control centers are sometimes, but not always, physically near the system itself.

Table 4.1
Potential Target Locations Across Layered Security Areas

Layered Security	Potential Target Locations
Perimeter areas	Access routes and pathways to ground-level stations, elevated infrastructure (including bridges) to elevated stations and tracks, and tunnel entrances
	Underground infrastructure
	Ground-level tracks and railroad crossings
	Exterior of operation-control center or building where center is located
	Area adjacent to exterior of system's power-generation plant
Exterior areas	Station interiors from entrances to ticketed-passenger entry points
Interior areas	Station interiors beyond ticketed-passenger entry points to train platforms
Restricted areas	Rail-operation, maintenance, service-support, and transit-security personnel's secured areas within stations
	Interior of system operation-control center
	Interior of system power-generation plant
Assets	Trains

interviews, all parties are generally interested in improving passengers' security, minimizing disruption in operations from potential terrorist attacks, and preventing or reducing the more frequent crimes at these more external locations. Therefore, we opted for opening the trade space of potential SIO solutions across a broader set of potential, perimeter, terrorist-attack locations.

We also made a distinction between the exterior and interior security layers and the physical separation within the stations. Even though the majority of security measures that we observed during our site visits appeared to be quite similar within the stations' concourses, corridors, and elevators leading to the train platforms, we defined the physical area from the infrastructure entrances through each station's concourse ticketing area to the passengers pass through the fare-card entry points as the *exterior layer*.

These exterior layer physical locations are separate from the rest of each stations' *interior layer*, which is defined as the rest of the concourse area after the passengers go through the fare-card entry points, and includes the corridors, stairwells, elevators, and escalators leading to and including the train platform areas located with each rail station.

We defined rail system facilities and the rooms occupied by rail operations and security personnel located at each station as the *restricted access layer* areas within our notional rail system.

Even though we used the term *security layers* in our study to refer to specific physical locations across the rail system, we also recognize that the security community has referred to implementing layers of security measures within the same physical layer where, for example, uniformed officers are on duty at one of the entrances to an underground station to enforce the no-parking zone of vehicles parked curbside directly in front of one of the street entrances to the station. In addition, and as a second layer of security, bollards are also in place along this perimeter area to increase the standoff distance and minimize potential passenger fatalities at the entrance or inside the concourse area of the station in the event that a suspicious vehicle does not immediately move away and a car bomb goes off at this location.

In Chapter Five, we include this definition and use of layers of security measures as part of our assessment of SIOs within each physical layer of our notional rail system and within a section in Chapter Five as part of the description of the interdependence across SIOs.

CHAPTER FIVE

Cost-Effectiveness Assessment of Security-Improvement Options for the Notional Rail System

Introduction

DHS, the U.S. Department of Transportation (DOT), and other federal, state, and local agencies have taken some steps to enhance rail and transit security since the 9/11 attacks. They have taken these steps in partnership with the public and private entities that own and operate U.S. rail systems. The international rail community has undertaken similar efforts.

Examples of initiatives that have been implemented or considered include threat and vulnerability assessments; screening programs; public education and awareness; perimeter barriers, high-tech fencing, and lighting; intrusion-detection equipment; alternative external-communication capability for continuity of operations; increased number of uniformed and undercover patrols on light rail and subway systems; hazmat training for personnel; increased number of inspections of trash receptacles and other storage areas; increased number and frequency of bomb-detecting canine teams; increased video surveillance and review of surveillance footage; and procurement of personal protective equipment for emergency responders.

In conducting our cost-effectiveness assessment, we gathered as much information as possible about domestic and international mitigation strategies, their potential effectiveness, and their estimated costs. Consistent with our research process for identifying and assessing attack scenarios, our approach focused on obtaining information from the site visits, key respondent interviews, and secondary-source material. This included measures in place *before* attacks occurred, which may have affected the likelihood of a successful attack, as well as how measures were altered after the attacks. We recognized that security measures effective in other countries may not, in themselves, be applicable to the United States. Since terrorists innovate and change tactics, security measures should also be continually developed to counter new threats. We therefore considered additional mitigation strategies that perhaps have not yet been implemented. Of course, multiple security measures may contribute to reducing the risk of any single attack scenario, and a single security measure implemented across the entire system of potential attack locations may contribute to reducing overall system vulnerabilities against the risk associated with many different attack scenarios.

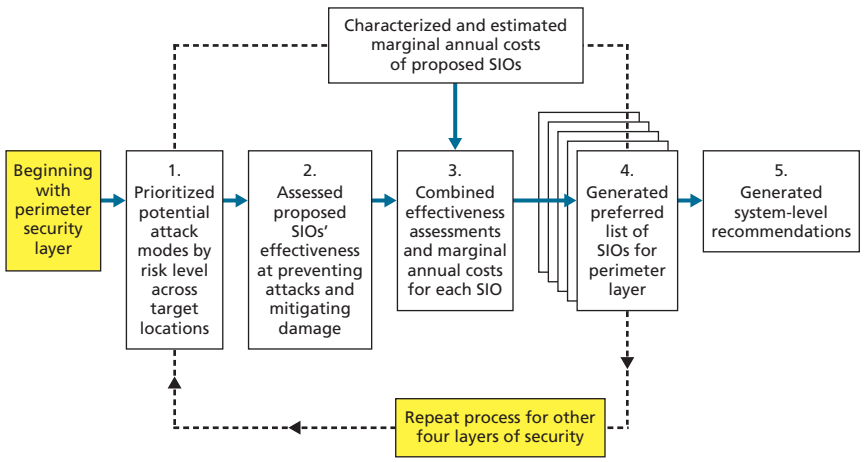
We combined insights from the risk assessment and identification of mitigation strategies to assess the costs and relative effectiveness of each strategy relative to reducing the risk of different attack scenarios. This required determining the likely impact of each mitigation strategy on reducing each risk and estimating the cost of each SIO. Through this process, we estimated costs for implementing and sustaining each strategy relative to its likely outcome or level of relative effectiveness against one or more of the terrorist-attack scenarios.

Assessment-Process Overview

Before we began the cost-effectiveness assessment process, we first characterized and estimated the marginal annual costs of all the proposed list of SIOs that are *not* part of the baseline set of security measures currently operating within the notional rail system (which were both described in Chapter Four). The cost elements and estimates for each SIO are provided in the next section with further details on the basis of estimates included as part of Appendix B.

Along with the estimating SIO marginal costs, Figure 5.1 displays the five steps of the specific assessment process that we developed as an analytical framework for generating a recommended set of SIOs, with the objective of prioritizing and ranking each option by assessing the greatest *relative improvements in overall effectiveness* at the lowest *marginal annual costs*. The five steps are summarized below with further discussions provided for each step in the sections that follow within this chapter.

Figure 5.1
Cost-Effectiveness Assessment Process



RAND *MG705-5.1*

Starting with the perimeter security layer, we first prioritize the potential attacks made by the aggregate level of assessed risk across each of the unique target locations within the perimeter (step 1 in Figure 5.1). We take the eight potential attack modes and the high to low risk levels of attacks at each of the 11 target locations previously (displayed in Figure 3.2 in Chapter Three) and map each unique perimeter-layer target location.

As shown in step 2 in Figure 5.1, for each potential attack mode and unique perimeter target location, we separately evaluated the *relative effectiveness* or impact each proposed SIO has if implemented over the current baseline security measures across the following two categories and four metrics:[1]

- *preventing* the potential attacks from occurring expressed in terms of *reducing the probability of occurrence*
- *mitigating damage* from the attack occurring expressed in terms of *averting potential fatalities, reducing recovery time* before rail operations are resumed, and *minimizing* economic consequences from the attack in terms of reducing the potential *loss of rail-system operating revenues*.

We next combine the set of relative effectiveness-rating results for each one of the four metrics into one overall assessment-rating value for each proposed SIO, and then divide each value by the estimated marginal annual costs (step 3 in Figure 5.1).

We then generate a preferred and ranked list of SIOs for this perimeter layer based on resulting overall effectiveness-per-dollar ratios and a template decision matrix described later in this chapter (step 4 in Figure 5.1).

These five steps of the assessment process are conducted again with the exterior security layer and the three other physical layers, ending with the innermost layer of rail-system assets being the protection of passengers' security on the trains (step 5 in Figure 5.1). For each physical security layer, we derived a preferred, prioritized list of the most cost-effective SIOs.

The list of preferred SIOs for each of the five layers is used along with other information to perform a system-level assessment and generate system-level SIO recommendations. More specifically, we create a security portfolio that differentiates SIOs based on their cost-effectiveness relative to their average marginal annual costs, which helps to account for real-world affordability (total cost) constraints. This is one of many ways in which the list of SIOs can be contextualized and subsequently prioritized. This final step in the assessment process and other practical issues to consider in determining a system-level portfolio of recommended SIOs are discussed in more detail later in this chapter.

[1] Other categories (such as apprehending terrorists) and metrics (such as minimizing economic loss to the region) could also be considered, but data limitations precluded us from formally including them in the present analysis.

Characterizing and Estimating Costs of Security-Improvement Options

We have grouped a proposed list of SIOs into three different types: process-based improvements, technology-based alternatives, and facility (or infrastructure) modifications. Each type is characterized by the relative magnitude of total investment and annual recurring costs and the inherent technical risks and uncertainties in predicting the expected levels of operational performance and accurately estimating these costs. For comparison purposes, Table 5.1 lists our assessment of the ability to predict operational performance and the level of uncertainty in the cost estimates for the three types of SIOs. Table 5.2 describes the specific SIOs used and the associated marginal cost range estimates.

All costs listed are in 2007 constant-year dollars. The first column lists the *investment cost*, which is an estimate of the one-time capital and other expenditures for procuring and, where applicable, testing and installing the security measures. The second column is the *annual recurring cost*, which is an estimate of the average annual expenses for additional personnel and, where applicable, the training, maintenance, spares, and upkeep of employing the security measures over their expected useful lives. The right column lists the *marginal annual cost*, which essentially is the annual life-cycle cost (based on a five-year time horizon) that accounts for both investment and recurring operating costs.[2] The marginal annual estimates represent the additional costs above and beyond the existing *baseline security measures (i.e., patrols and systems) that are currently in place* within the notional rail system. Since the estimates are based on the number and mix of ground, elevated, and below-ground stations, the number of rail

Table 5.1
Comparisons of Security-Improvement Option Types

Type of SIO	Predicting Operational Performance	Estimating Uncertainty
Process-based improvements	Difficult to quantify on-the-job improvements	Very low
Technology-based alternatives	Varies depending on amount of field data collected	Depends on technology readiness level (TRL)[a]
Infrastructure or facility modifications	Field test (e.g., hardening, lethality) data available	Low

[a] The DHS Science and Technology Directorate adapted, from NASA, nine TRLs with values from 1 to 9 with specific criteria for assessing the developmental maturity of a technology-based security system or device within a system, from basic research (TRL 1) through production and deployment (TRL 9). Further information is provided in the chart "Homeland Security Program Management Model for Technology Readiness Level (TRL) Assessment" (see DHS, 2005).

[2] We amortized the up-front investment over a five-year period by applying a 7 percent annual factor compounded over five years and dividing by five. We then added the annual recurring-cost estimates, which is the average expenses incurred per year over this first five years.

Table 5.2
Marginal Costs of Three Sets of Security-Improvement Options

SIO	Description	Investment Cost ($ millions)	Annual Recurring Cost ($ millions)	Total Marginal Annual Cost ($ millions)
Process-based improvements				
1.0	Implementing enhanced security training	0	0.08–0.20	0.08–0.20
2.0	Adding canine team	0.18–0.33	0.51	0.56–0.70
3.0	Instituting employee background checks and issuing updated badges	0.002	0.06	0.06
4.1	Increasing the number of signs in stations and rail vehicles and the frequency of public-address announcements	0	0.04	0.04
4.2	Installing LED displays with updated passenger-rail status in stations	0.38–0.75	0.04–0.08	0.14–0.29
Technology-based alternatives				
5.0	Installing perimeter fencing and intrusion-detection systems (IDSs) adjacent to ground-level tracks	2.4–7.6	0.7–2.8	1.4–4.9
6.0	Installing stationary passenger- and baggage-screening systems in stations	0.38–0.75	0.04–0.08	0.14–0.29
7.0	Using mix of portable (handheld) explosive or chemical and biological detection systems	0.68–1.60	0.18–0.41	0.37–0.86
8.0	Installing perimeter fencing and adding perimeter surveillance systems adjacent to ground-level tracks	4.9–13.3	0.77–3.64	2.1–7.4
8.1	Installing tunnel surveillance system	1.7–6.2	0.61–3.28	1.1–5.0
9.0	Adding rail-vehicle surveillance systems	3.0–5.5	0.16–0.21	1.0–1.7
10.0	Upgrading personnel access-control systems (ACSs) in all restricted areas	0.85–3.2	0.25–1.4	0.5–2.3
11.0	Implementing hybrid security systems in stations	4.5–31.0	0.45–6.2	1.7–14.9
Facility or infrastructure modifications				
12.0	Installing blast-resistant containers in stations	0.75	0	0.21
13.1	Installing fixed blast barriers curbside adjacent to stations' street entrances and exits	3.2–4.2	0.16–0.24	0.9
13.2	Installing retractable bollards at rail operation-control center building and rail power-plant entrances and exits	0.10	0.01	0.03
14.0	Installing pillars to elevated infrastructure supporting elevated stations and tracks	0.6–1.3	0	0.17–0.36

cars, track length, and the like, the *actual cost of investing in and the recurring cost of implementing each of these SIOs for other operational rail systems may vary considerably from these range estimates.*

We provide brief examples of the cost-estimation process for each type of SIO. Further details on the basis of the range estimates, uncertainties, cost references, and more information about all the SIOs are provided in the first section of Appendix B.

Process-Based Security-Improvement Options: Implementing Enhanced Security Training

The investment cost is the one-time cost of developing training materials for conducting security-awareness seminars, tabletop workshops, games, drills, and full-scale exercises. The content of the training materials ranges from providing instructional information on detecting improvised explosive devices (IEDs) to handling evacuations after locating suspicious, unattended packages and emergency procedures in response to exposure of passengers to chemical-based weapons, dirty bombs, and other methods.

The annual recurring cost is based on the estimated expenses for (1) paying one full-time training coordinator and a part-time staff member (at $60,000 each) and (2) the training material and other costs incurred per session (ranging from $1,500 to $70,000) and (3) is driven by the number and type of sessions projected over an assumed three-year cycle based on the average class size and mix of rail operators and security personnel per class (varying from 25 to 225) for training the total staff of 2,000 people.

Technology-Based Security-Improvement Options: Installing Perimeter Fencing and Intrusion-Detection Systems Adjacent to Ground-Level Tracks

The investment cost is the one-time cost of procuring and installing (1) standard fencing with barbed or razor wire on top adjacent to the 30 miles of ground-level track at between $2 and $5 per linear foot, (2) IDSs in the form of either fence-mounted sensors at between $5,000 and $20,000 each or underground sensors at $20,000 each based on a quantity of 320 installed every 500 feet over the 30 miles of fencing, and (3) cables along the 30-mile perimeter connected to two workstations within the rail operation-control center at $3 per linear foot. A TRL value of 9 was assessed for both fence-mounted and underground intrusion-detection sensors, as these systems have completed production and the costs are based on vendor quotes. The average recurring cost is based on the total expense of maintaining the fencing and cables (at approximately 10 percent of the total investment cost per year) over a 10-year service life and IDS sensors at between 20 and 30 percent of the total investment cost per year over a five- to 15-year service life. We assumed that the rail security personnel assigned to the operation-control center would be available to staff the colocated perimeter IDS-monitoring workstations.

Infrastructure- or Facility-Modification Security-Improvement Options: Installing Blast-Resistant Containers in Stations

The investment cost is the one-time procurement and placement of 190 blast-resistant containers across all 47 stations in the notional rail system at a unit cost of $3,900 each. There is very minimal annual recurring cost estimated, since the rapid-response force (in particular, the hazmat team) and rail operators are assumed to be available and trained in emergency procedures to properly use these containers in handling the disposal of potentially hazardous, unattended packages.

Perimeter-Layer Cost-Effectiveness Assessment Process

We now turn to illustrating the five cost-effectiveness assessment steps that were initially displayed in Figure 5.1. We begin with the perimeter security layer. The process for each layer is detailed in a separate section of Appendix B.

Prioritize Attack Scenarios by Level of Assessed Risk

We first prioritize and focus on the same eight terrorist-attack scenarios assessed as high risks (displayed in Figure 3.2 in Chapter Three) that are associated with the perimeter layer (step 1 in Figure 5.1). Table 5.3 lists the eight unique types of potential target locations (as column headings) within the perimeter layer across the eight potential terrorist-attack modes (as row headings).[3] Table 5.3 reproduces the same high-risk–level terrorism results for each attack scenario.

Table 5.3 displays an eight-by-eight matrix representing the possibility of a total of 64 attack modes (or cells) at unique types of perimeter target locations where a terrorist incident can occur. However, shown by blank cells, 41 possible attacks at unique types of perimeter target locations were considered medium- or low-risk incidents or not relevant based on the results of the threat, vulnerability, and consequence assessments described in Chapter Three.

The remaining 23, or 36 percent, have been previously assessed as high risk over five out of the eight possible attack modes listed in the left column.

The risk assessed within each cell displayed in Table 5.3 provides a basis for establishing a priority ranking for each of the eight terrorist-attack modes based on the total number of unique perimeter target location types (23) assessed as high risk (across each row) relative to the others. We elected to weight the number of high-risk occurrences by the number of unique types of perimeter locations rather than using the actual number of possible physical locations (e.g., a total of 50 entrances—two per station—at each of the 25 underground stations within our notional rail system). This method

[3] As part of the notional rail system, the two right columns in Table 5.3 replaced the single right column illustrated in Figure 3.2 in Chapter Three for assessing potentially different SIOs for the perimeter entrance and exit areas around the rail-system operation building and the power-plant infrastructure.

Table 5.3
Risk-Assessment Summary Across Perimeter Locations (item 1 in Figure 5.1)

Terrorist-Attack Scenario	Underground Station Access and Pathways	Underground Infrastructure	Ground-Level Station Entrances	Ground-Level Rail Infrastructure	External Attack on Ground-Level or Elevated Train	Elevated Station Infrastructure	Entrances and Exits to Rail-System Operation Center Building	Entrances and Exits to Power-Plant Infrastructure	High-Threat Occurrences
Vehicle bombs[a]	High		High	High	High	High	High	High	7
Small explosives	High		High		High		High	High	5
Large incendiary			High		High				2
Small incendiary									0
Armed attack	High		High		High				3
Unconventional weapon									0
Sabotage		High		High	High	High	High	High	6
Hoax									0
Total									23

[a] Vehicle bombs are equivalent to the large-explosive terrorist attack in Figure 3.2 in Chapter Three.

accounts for our focus on assessing each proposed SIO on the improved effectiveness at preventing or mitigating damage against a single, specific attack mode (e.g., vehicle bombs) at a single unique type of perimeter location over the number of locations (e.g., the likeliest number of underground station entrances) at which this type of attack could take place.[4]

For example, vehicle bombs (or, in general, large explosives) are assessed as high risk for all but one type of perimeter location, compared to a potential large incendiary attack assessed as a high risk at only two types of perimeter locations. The total number of high-risk occurrences for each terrorist-attack scenario is listed in the far-right column of Table 5.3.

The total number of high-risk occurrences (23) is important, since it is used in the next two assessment-process steps as the basis for generating an effectiveness-rating value (step 2) for each proposed SIO at preventing and mitigating damage across five out of a possible eight high-risk attack scenarios. As a result, we focus the effectiveness assessments for this perimeter layer on attack modes considered high risk and did not consider the three other attack modes identified as medium or lower risk: small incendiary, unconventional weapons, and hoaxes.

Assess Relative Effectiveness of Security-Improvement Options

Preventing Terrorist Attacks. Next, we assess the effectiveness of the perimeter layer SIOs capable of preventing attacks from occurring and mitigating the resulting damage (step 2 in Figure 5.1). The objective of this step in the effectiveness process is to quantify or, at best, qualify the relative impact that each security measure has on reducing the likelihood or probability of an attack occurring over the current set of baseline security measures in an internally consistent way.

We assessed each SIO on its ability to detect a potential attack before it occurs as a direct way to reduce the probability of the incident taking place. For example, there are field performance data on the ability of trained and certified canine-and-patrol-officer teams to positively detect specific types of bomb residue and explosive particles on passengers and their packages (SIO 2.0; see Table 5.2 for list of SIOs). In addition, well-documented reports address the performance characteristics of the five other technology-based alternatives: installing IDSs with alarms and motion sensors either mounted on perimeter fencing or placed underground (SIO 5.0) or perimeter surveillance systems installed around perimeter fencing adjacent to ground-level tracks (SIO 8.0) and in the tunnels (SIO 8.1); using portable (handheld) detection devices (SIO 7.0); and installing sensors or alarms on fixed, curbside blast barriers and retractable bollards (SIOs 13.1 and 13.2). Further information on the detection-assessment capa-

[4] Even though the focus of the assessment for each SIO (e.g., installing curbside barriers) is on the effectiveness against a single, specific attack mode (e.g., vehicle bomb), we do use the number of potential physical target locations as the basis for estimating the total annual marginal (procurement, installation and recurring) costs for each option.

bility of canine teams and the other technology-based alternatives is provided along with cited references in the second section of Appendix B.

Even with confident and known detection-performance data across the SIOs, the full value of preventing attacks from occurring will also require the e*nhanced training* necessary for providing rail-security personnel with the critical skills needed to fully utilize the maturer technology-based alternatives and instructing them on the operation-control center's, line's, and station's sets of operational procedures and communication protocols for being able to *quickly respond* to apprehending terrorists and disarming weapons. In addition to the ability to detect a potential attack and preventing it from taking place, we included an assessment of the deterrence value of placing fixed blast barriers along the curbside of ground-level and underground station entrances as well as retractable bollards at the entrances to the rail-system operation-control center and power-plant facilities (SIOs 13.1 and 13.2). These two SIOs provide deterrence value to the extent that increasing standoff distances and reducing the potential blast radius from a vehicle bomb located curbside will discourage terrorists from carrying out these attacks around rail stations' street-level entrances and passageways and near entrances and exits where the operation-control center and rail power-plant facilities are located. We also made a qualitative assessment of the two process-based security measures for implementing enhanced security training (SIO 1.0) and performing background investigations and issuing new badges for all the rail employees (SIO 3.0) to reduce the likelihood of an attack occurring from a deterrence perspective.

As an effective deterrent against terrorist attacks, enhanced security training can be geared to increased uniformed presence either on a regular basis or as part of field exercises to randomly deploy a rapid-response security team to potential target locations across the notional rail system, focused on disrupting terrorists' plans. According to case-study interviews that we conducted, rapid-response teams can serve to deter or, at a minimum, discourage a terrorist from using a particular attack mode at a particular location, especially if these security teams are randomly deployed to different potential target locations to augment the station's security force during their daily patrols of the concourse and platform areas.

Likewise, the implementation of background investigations on all rail employees (operators and security officers) serves to identify and dismiss those with previous criminal records. This could reduce the potential for terrorist attacks of sabotage and hoaxes, since a terrorist group might compromise them or they could be likelier suspects providing access to restricted areas and disclosing other insider information than would employees with no criminal offenses.

Keep in mind that the value of deterrence assessed across SIOs does not entirely encompass preventing an attack from occurring throughout the rail system, but it is also related to the potential to force terrorists to consider use of other tactics—different attack modes at different target locations. *Therefore, assessing the effectiveness at prevent-*

ing attacks from taking place has to first look at detection, while still including deterrence from an overall value-added perspective.

Table 5.4 lists the assessment for each of the proposed SIOs capable of preventing attacks from occurring across the five terrorist-attack modes identified as high risk for each unique target location within the perimeter area. (SIOs not listed are assessed as having no relative effect at preventing attacks over the baseline set of security measures.)

For each SIO, we established a relative assessment rating for each of the five terrorist attacks listed in each cell, with an integer value of 1 for low effectiveness, 2 for moderate effectiveness, and 3 for high effectiveness. An assessment of very low is represented by a cell value of 0.5. Blank cells indicate that we assessed the perimeter-layer SIO not to be relevant for preventing a specific terrorist attack from occurring. (We also left cells blank in the other effectiveness-assessment tables in this section where the specific SIO is assessed as not relevant at impacting one of the other effectiveness metrics.) In addition, a negligible rating in Table 5.4 (and other tables in this section) indicates that there is an implicit, not explicit, assessment that the SIO was minimally effective at preventing an attack from occurring (or, for the other tables, at mitigating the damage in terms of the other effectiveness metric), which we could not substantiate or validate over the course of this study through site-visit interviews and reports. Therefore, no numerical minimum-rating value could, with confidence, be assigned.

Next, the prevent-attack assessment-rating values for each SIO are computed and listed in the far-right column of Table 5.5 by doing the following:

- setting numerical values for each qualitative assessment listed (for cells across each row) using the above numerical rating-value guidelines
- taking the weighted average by multiplying each SIO value (column headings) listed by the total number of occurrences previously assessed as high risk at unique perimeter locations for each attack mode (as values in the top row, which are the same ones previously listed in the far-right column of Table 5.3)
- adding the results across each of the five potential terrorist-attack modes
- dividing this total value by the total number of unique high-risk locations across all five attack modes of 23 (see Table 5.3).[5]

The calculations for this step in the assessment process could produce an overall rating value ranging from 0 (for an SIO with no effect on any of the five high-risk attack scenarios) to 3 (for one rated as high across all scenarios). The weighted average prevent-attack rating value for each SIO is the same analytical method that we applied

[5] We chose to use the weighted average rather than the average as the assessed values across each SIO for the effectiveness-rating computations discussed here and later in this section to account for and factor in the different unique target-location types terrorists can potentially select within the perimeter (and the other security layers) for a specific attack.

Table 5.4
Assessment of Perimeter Security-Improvement Options Preventing Terrorist Attacks from Occurring

Proposed SIO	Description	Vehicle Bombs	Sabotage	Small Explosives	Armed Attack	Large Incendiary
1.0	Enhanced security training		Low	Low	Low	
2.0	Canine teams	Very low		Low		
3.0	Employee background checks		Low	Low	Low	
5.0	Perimeter fencing and IDSs		Moderate	Low	Moderate	
7.0	Portable (handheld) detection systems	Very low		Low		
8.0	Perimeter fencing and surveillance systems		Moderate	Low	Moderate	
8.1	Tunnel surveillance system		Low to moderate			
13.1	Fixed blast barriers	Moderate		Very low	Negligible	Low
13.2	Retractable bollards	Moderate		Very low	Negligible	Low

for computing the rating values for each SIO for the other three metrics used and described next for assessing the effectiveness of mitigating damage from the same five high-risk attack modes.

Mitigate Damage from Terrorist Attacks. Next, we evaluate how severe the relative damage from each of the potential terrorist attacks would be after implementing each one of the perimeter-layer SIOs that are capable of mitigating damage. For each SIO, the relative effectiveness of mitigating damage from an attack is based on combining the assessment results of three metrics—averting fatalities, reducing recovery times until operations can be resumed, and minimizing the loss of rail-system operating revenues—over staying with the baseline set of security measures. Although not a formal part of our analysis, we conclude this section with a discussion of minimizing economic losses to businesses.

Averting Fatalities. For our notional rail system operating with the baseline set of security measures, we first qualified the potential number of *benchmark* fatalities based on our assessment of expected outcomes across specific attacks at unique types of perimeter target locations based on a combination of reported data on, for example, the size (TNT yields) of weapons (from small explosives to vehicle bombs), the effective blast radius effects, and the density of passengers estimated within or near rail-system infrastructure within the blast radius area (the latter where debris could cause additional fatalities).

For example, a small explosive or, specifically, a backpack-sized bomb (with a TNT yield of 50 lbs.) detonated on the sidewalk directly adjacent to the main entrance

Table 5.5
Perimeter Security-Improvement Option Assessment Ratings for Preventing Terrorist Attacks from Occurring

Proposed SIO	Description	Unique Types of Locations Assessed as High Risk					Prevent-Attack Rating
		Vehicle Bombs (7)	Sabotage (6)	Small Explosives (5)	Armed Attack (3)	Large Incendiary (2)	
1.0	Enhanced security training		Low	Low	Low		0.6
2.0	Canine teams	Very low		Low			0.4
3.0	Employee background checks		Low	Low	Low		0.6
5.0	Perimeter fencing and IDSs		Moderate	Low	Moderate		1.0
7.0	Portable (handheld) detection systems	Very low		Low			0.4
8.0	Perimeter fencing and surveillance systems		Moderate	Low	Moderate		1.0
8.1	Tunnel surveillance system		Low to moderate				0.4
13.1	Fixed blast barriers	Moderate		Very low	Negligible	Low	0.8
13.2	Retractable bollards	Moderate		Very low	Negligible	Low	0.8

of one of the underground rail stations has the potential to kill everyone within 13 feet and 50 percent of the passengers between 13 and 20 feet away. Further details on the factors that affect the magnitude and range of potential fatalities (and injuries) for this terrorist scenario and various other explosive weapon–related attack modes at the perimeter and other security layer locations are provided in the third section of Appendix B.

For unconventional chemical or biological weapons, assessment of the magnitude of potential fatalities is based on, for example, a likeliest estimate of the effected size of exposed area impacted, the type of environment (e.g., enclosed, vented, open) in which the attack originated, the elapsed exposure time, and the density of passengers within that area over this exposure time.[6]

For the notional rail system operating with the baseline set of security measures, we used the fatality (and damage) assessment information along with the comparative consequence outcome data used as part of the risk-assessment process[7] (discussed in Chapter Three) as the basis for qualifying the magnitude of potential fatalities across each attack mode and unique type of perimeter target location. From this information, we estimated comparative relative consequences, which we divided into three rating categories:

- *low* represents up to two fatalities
- *moderate* represents between three and seven fatalities
- *high* represents more than eight fatalities.

Table 5.6 provides our benchmark qualitative assessment of the magnitude of potential fatalities for each of the five high-risk attack modes across the eight unique type of perimeter target locations for our notional system operating with the baseline set of security measures.

Even though there is a higher likelihood of vehicle bombs being set off at curbside locations directly in front of entrances and passageways to rail stations, the magnitude of potential fatalities from an armed attack was almost on par with fatalities caused by vehicle bombs. Similar benchmark comparative results of the differences in the magnitude of fatalities across attack scenarios were based not only on differences in the likelihood of the attack occurring at specific target locations but on differences in blast

[6] Further information on the magnitude of potential fatalities from unconventional weapons can be found in various open sources, such as EPA (2007), Monterey Institute of International Studies (undated[b]), and Wenck et al. (2007).

[7] As part of the risk-assessment process discussed in Chapters Two and Three, we used the summary-level consequence information to provide only *relative comparisons* of the different magnitude of average fatalities (and injuries) incurred from the terrorism database across previous rail attacks and tactics that have been staged to date. The average number of fatalities by terrorist tactics could not be used in an absolute sense, since it is based on specific incidents at rail systems with varying levels of complexity and, even though representative, is not directly applicable as a *quantitative argument* for projecting the magnitude of potential fatalities for our notional system.

Table 5.6
Benchmark Magnitude of Fatalities Assessed Across the Perimeter Layer

Attack Scenario	Underground Station Access and Pathways	Underground Infrastructure	Ground-Level Station Entrances	Ground-Level Rail Infrastructure	External Attack on Ground-Level or Elevated Train	Elevated Station Infrastructure	Entrances and Exits to Rail-System Operation Center Building	Entrances and Exits to Power-Plant Infrastructure
Armed attack	Moderate to high		Moderate to high		Moderate to high		Moderate	Low to moderate
Vehicle bombs	High		High	Moderate to high	High	High	Moderate to high	Moderate to high
Small explosives	Moderate	Moderate	Moderate		Low to moderate	Moderate	Moderate	Moderate
Sabotage		Low to moderate		Low to moderate	Low to moderate	Low	Low to moderate	Low to moderate
Large incendiary	Low		Low to moderate		Low		Low	Low to moderate

radius and lethality of the type of weapon used, the standoff distance to the target, and the nominal to peak rush-hour passenger density levels at locations within the notional rail system at the time of the attack.

Table 5.7 lists the assessments for each of the proposed perimeter-layer SIOs with potential to avert (or minimize) fatalities across the five attack modes identified as high risk for each unique target locations within the perimeter area. For each SIO, we established a relative effectiveness rating for averting fatalities compared to the benchmark magnitude of fatalities listed in Table 5.6 for the notional rail system operating with the baseline set of security measures. The rating for averting fatalities was divided into three categories and values, where a proposed SIO was assessed as follows:

- *low* effectiveness rating, indicating capability of averting only one fatality with a value of 1
- *moderate* effectiveness rating, indicating capability of averting between two and three fatalities with a value of 2
- *high* effectiveness rating, indicating capability of averting four or more fatalities with a value of 3, compared to staying with the baseline set of security measures.

To illustrate the assessment process, we assessed the relative effectiveness of implementing SIOs for averting fatalities for the same terrorist scenario described above of detonating a small-explosive, backpack-sized bomb on the sidewalk directly adjacent to the main entrance of one of the underground stations. Deploying canine teams (SIO 2.0) to this potential perimeter target location may result in either or both of the following:

- moving the terrorist with the backpack bomb away from this ideal sidewalk location where he or she would prefer to stage the attack
- forcing the terrorist to deploy another tactic, with the knowledge that the use of canine teams can be an effective countermeasure at detecting explosive particles on the terrorist or backpack that he or she is carrying.

Even though the terrorist could still detonate the bomb, the movement of the terrorist away from the main entrance can reduce the number of potential fatalities by increasing the standoff distance of passengers from the effective blast radius area. Even though the installation of blast barriers (SIO 13.1) at curbside locations adjacent to the main entrances of underground stations may serve to reduce the magnitude of potential fatalities of passengers (and damage to rail facilities and infrastructure) within or outside of the blast radius of vehicle bombs, a similar impact on averting fatalities from small backpack bombs is almost negligible.

Table 5.7
Assessment of Perimeter Security-Improvement Option Effectiveness in Averting Fatalities

Proposed SIO	Description	Unique Types of Locations Assessed as High Risk					Averting-Fatality Rating
		Vehicle Bombs (7)	Sabotage (6)	Small Explosives (5)	Armed Attack (3)	Large incendiary (2)	
2.0	Canine teams	Low		Low			0.5
5.0	Perimeter fencing and IDSs		Very low to low	Low	Low		0.5
7.0	Portable (handheld) detection systems	Low		Low			0.5
8.0	Perimeter fencing and surveillance systems		Very low to low	Low	Low		0.5
8.1	Tunnel surveillance system		Low				0.3
13.1	Fixed blast barriers	Moderate		Low to moderate	Low	Very low	1.1
13.2	Retractable bollards	Moderate		Low to moderate	Low	Very low	1.1
14.0	Structurally reinforced pillars	Moderate to high		Moderate			1.2

Across these two options and as a further crosscheck on these two options, installing blast barriers (SIO 13.1) is negligible at averting fatalities compared to deploying canine teams (SIO 2.0). Furthermore, when compared to security using portable (handheld) detection systems (SIO 7.0), canine teams (SIO 2.0) may prove slightly more effective at averting potential fatalities based on more positive detections and fewer false alarms.

The qualitative assessments for averting fatalities for these and all the other SIOs across the potential attacks are summarized in Table 5.7, along with the rating values for each SIO listed in the far right column. As previously described, each averting-fatality rating value was generated by first setting numerical values for each qualitative assessment using the rating guidelines set above, multiplying each value by the number of unique types of perimeter locations assessed as high risk, summing these products, and then computing the weighted average by dividing the total value by the same total number of unique perimeter locations of 23 (sum of the values listed in the top row) across the same five potential attack modes.

Reducing Recovery Times. Next and similar to the assessment for fatalities averted, we first established a benchmark set of guidelines for assessing the projected recovery times until operations are resumed across each attack mode and at unique types of perimeter target locations for the notional rail system operating with the baseline set of security measures. Based on an estimate of the physical damage incurred from the attack,[8] the guidelines assume that the costlier the damage, the more (in a nonlinear way) estimated time it will take to rebuild, reconstruct, and do the repairs needed before rail-system operations can be fully resumed.

We estimated the expected recovery times based on the magnitude of severity and estimated cost of the total physical damage for each specific attack at one of the unique types of perimeter target locations and categorized them into one of the following three brackets:

- *low level of physical damage cost* estimated at *less than $1 million* with an expected recovery time of between three and 10 days
- *moderate level of damage* estimated at *between $1 million and $10 million* with an expected recovery time of between 10 days and two months
- *high level of damage* estimated at *greater than $10 million* with an expected recovery time of between two and six months.

For each of the high-risk attack modes assessed for each unique type of target perimeter location, we estimated a rough order-of-magnitude (ROM) cost of the physi-

[8] We estimated physical damage from a terrorist attack while operating under the same baseline set of security measures (without adding hardening or other mitigating measures) as the cost (in current dollars) estimated for cleaning up (especially in the case of an unconventional chemical or biological attack), reconstructing, and repairing the facilities and infrastructures of the notional rail system to their original condition.

cal damage at the fidelity needed to fit into one of the three levels of physical-damage cost brackets listed above based on an assessment of the following:

- the severity of the attack in terms of the potential standoff distances and effective blast radii associated with attacks caused by vehicle bombs, small explosives, and large and small incendiary modes (with further information and cited references provided in the third section of Appendix B)
- the magnitude of the cost of clean-up (especially caused by attacks using unconventional chemical, biological, and similar weapons), reconstruction, and repair of specific rail facilities and infrastructures, using cited costs from past RAND research (Stevens, Schell, et al., 2004) and other reports on analogous infrastructure costs, the size of the construction labor force needed, and the total material costs incurred.

Depending on the specific location of the attack and the severity of the damage to *critical* facilities (e.g., the rail operation-control building or power plant), hub station or underground stations within close proximity of the city center, and elevated infrastructure supporting above-ground stations, we reduced the expected recovery-time range estimates to account for the likelihood that rail management will respond quickly to initiating actions (e.g., expediting approval of the capital funds needed, quickly soliciting and getting construction contractors on board) at minimizing the operational disruption and fully restoring operations to passenger service across the notional rail system.

Table 5.8 lists the benchmark recovery-time range estimates (in days) for each attack at and across each of the unique types of perimeter target locations for the notional rail system operating with the baseline set of security measures. We also listed our assessment of rail management's importance at promptly initiating recovery actions across each of the eight unique types of perimeter target locations (listed in the bottom row) that we identified as *critical* to minimizing disruptions in rail-passenger service. The average recovery-range estimates for each of the five attack scenarios are listed (in the far right column) and represent the average of the lower and upper values listed across those locations where the threat was previously assessed as high.

To illustrate the assessment process for reducing recovery times, we compared the effectiveness of two infrastructure-modification SIOs at being able to absorb the blast effects of a vehicle bomb detonated at the curbside directly in front of the load-bearing infrastructure supporting one of the elevated rail stations within the notional rail system. Installing barriers at this curbside location (SIO 13.1) as previously assessed could serve to influence terrorists to move the blast location to a less-than-ideal location, providing a greater standoff distance to passengers on the sidewalks at the main entrance leading up to the elevated rail station concourse, platform, rails, and potential trains crossing overhead. Not only do the barriers serve to avert some potential

Table 5.8
Benchmark Recovery Times (Days), Estimated Across the Perimeter Layer

Terrorist-Attack Scenario	Underground Station Access and Pathways	Underground Infrastructure	Ground-Level Station Entrances	Ground-Level Rail Infrastructure	External Attack on Ground-Level or Elevated Train	Elevated Station Infrastructure	Entrances and Exits to Rail-System Operation Center Building	Entrances and Exits to Power-Plant Infrastructure	Average Recovery-Time Range Estimate
Vehicle bombs	80–120		100–140	60–100	30–60	120–160	30–50	30–50	56–85
Small explosives	20–40		30–50		40–60		20–40	20–40	16–29
Large incendiary			10–30		20–40				4–9
Armed attack	3–6		6–10		6–10				2–3
Sabotage		10–30		3–6	3–5	10–30	3–5	3–5	4–10
Management importance for minimizing operational disruption	Significant at hub and underground stations within city center	Moderate to significant, depending on proximity to city center and hub station	Moderate to significant, depending on proximity to city center and hub station	Minimal to moderate, depending on distance to city center and hub station	Moderate to significant, depending on number of fatalities and injuries	Moderate to significant, depending on number of fatalities and injuries	As high as significant, depending on severity of physical damage	As high as significant, depending on severity of physical damage	

fatalities at the street level and above, but the steel-reinforced concrete structural composition of the barriers can absorb a portion of the vehicle-bomb blast effects and reduce the severity of the damage to the infrastructure (load-bearing pillars) supporting the elevated station.[9]

Comparatively, installing reinforced pillars spaced between the existing pillars of the elevated infrastructure (SIO 14.0) cannot prevent vehicle-bomb blasts from occurring and only slightly reduces the probability of the attack,[10] but it can potentially reduce the number of potential fatalities of passengers on an elevated station for which they are supporting the loads, minimize the recovery time by providing emergency responders easier access to injured passengers on the train platforms and other areas of the station, and potentially reduce the rebuilding time needed to resume rail operations.

Table 5.9 summarizes our assessment of the effectiveness of the proposed perimeter-layer SIOs capable of reducing the recovery times across each of the five attack modes identified as high risk for each unique target location within the perimeter area. For each SIO and potential attack, we established a relative consequence assessment rating for reducing recovery time:

- *Low reduction in recovery time* of two weeks (14 days) or less represents a rating value of 1.
- *Moderate reduction in recovery time* of greater than two weeks (14 days) and up to two months (60 days) represents a rating value of 2.
- *High reduction in recovery time* of greater than two months (60 days) over staying with the baseline set of security measures for the notional rail systems represents a rating value of 3.

A very low reduction in recovery-time assessment is represented by a rating value of 0.5.

For each SIO, a rating value for reducing recovery time across all five potential attacks was computed by first setting numerical values for each qualitative assessment listed (for cells across each row) using the guidelines just described, then taking the weighted average based on the total number of unique perimeter locations

[9] Several government agencies, such as the U.S. Army Corps of Engineers (2006) and the Naval Civil Engineering Laboratory (1988), have published the results of surface bomb blast testing the hardening effects of several commercial blast barriers against different size vehicle bombs. Naval Civil Engineering Laboratory (1988) includes information on vehicle barriers and blast survivability for buildings. It provides information to aid owners in protecting their property, assets, and personnel against terrorist vehicle bombs. This manual includes information on access control, vehicle barrier systems and testing, and sample blast-vulnerability analyses.

[10] If a terrorist cell recognized the recent addition of structurally reinforced concrete pillars, this option could serve as a deterrent measure to change the intended vehicle-bomb attack to a more vulnerable location.

Table 5.9
Assessment of Perimeter Security-Improvement Option Effectiveness in Reducing Recovery Times

Proposed SIO	Description	Unique Types of Locations Assessed as High Risk					Reduced Recovery-Time Rating
		Vehicle Bombs (7)	Sabotage (6)	Small Explosives (5)	Armed Attack (3)	Large Incendiary (2)	
2.0[a]	Canine teams	Very low to low		Low			0.4
5.0[a]	Perimeter fencing and IDSs	Low	Negligible	Very low	Negligible		0.4
7.0[a]	Portable (handheld) detection systems	Very low to low		Low			0.4
8.0[a]	Perimeter fencing and surveillance systems	Low	Negligible	Very low	Negligible		0.4
8.1[b]	Tunnel surveillance system		Very low				0.1
13.1[c]	Fixed blast barriers	Moderate		Moderate to high		Low	1.2
13.2[c]	Retractable bollards	Moderate		Moderate to high		Low	1.2
14.0c	Structurally reinforced pillars	High		High			1.6

[a] SIOs 2.0, 5.0, 7.0, and 8.0 were assessed as effective at reducing recovery times because each option serves to reduce the potential damage to the rail infrastructure and facilities by increasing the standoff distances from the target at which terrorists would ideally prefer to be staging their attack.

[b] SIO 8.1 was assessed as effective at reducing recovery times because it serves to quickly locate and identify the impact points of the attack, the severity and damage assessments of derailment, and how best to proceed forward with necessary repairs.

[c] SIOs 13.1, 13.2, and 14.0 were assessed as effective at reducing recovery times because each option serves to reduce the potential damage by both minimizing the blast effects of the explosive impact of each attack and increasing the standoff distances and the terrorists' preferred staging areas.

(values in the top row) for the same five attacks assessed as high risk. The reduced recovery-time rating values for each SIO are listed in the far right column in Table 5.9. In addition to the comparative assessment of the two SIOs described above, further information on the basis for the SIO assessments is listed in the table notes.

Minimizing Loss of Operating Revenues. To assess the effectiveness of each of the proposed perimeter layer SIOs in reducing the loss of rail-system operating revenues relative to each potential terrorist attack occurring at each unique type of target location across the notional rail system over staying with the baseline set of security measures, we first have to estimate, as a minimum, the total daily operating revenue of passenger fares collected, the total average number of passengers using the rail system each day, and the total number of passenger trips per day across all 47 stations.

Each potential SIO's effectiveness at reducing the economic consequences after each potential attack is expressed in terms of the estimated reduction (or improvement) in the projected economic loss of rail-operating revenues for the expected number of passengers per day who are not able to commute by rail.

For the notional rail system under normal operating conditions, with all five lines and 47 rail stations operating, we set the average number of weekday passengers per day at 200,000 and the average weekday rail-passenger trips per day at 340,000, based on passengers using the rail system for approximately 1.7 trips per day.[11] We set the average daily operating revenues for the notional rail system from passenger fares at $1.2 million per day, which computes to an average operating revenue of fares collected for each passenger commuting on the rail system at $3.55 per day.[12]

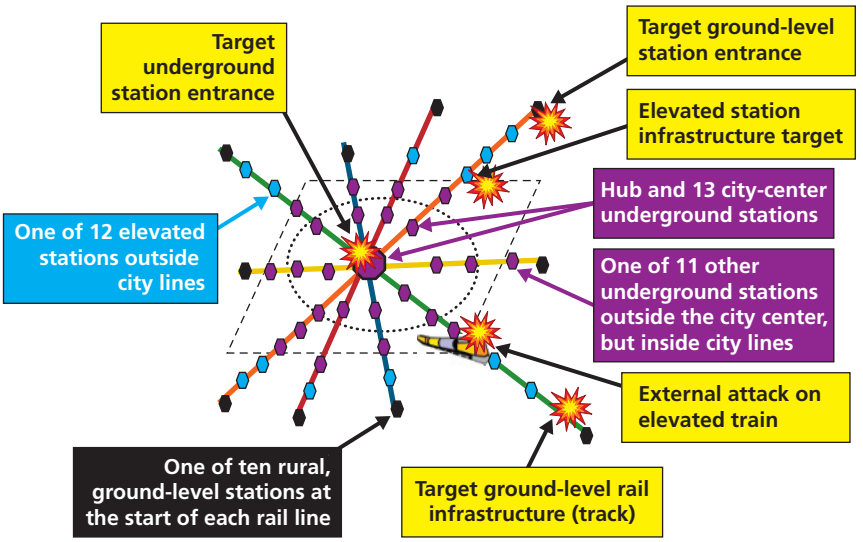
Figure 5.2 displays the notional rail-system network with the hub and 24 other underground stations (in purple) illustrated within and outside the city line (denoted by the blue dashed circle), the 12 elevated stations (in blue) in the suburbs outside the metropolitan area (denoted by the black dashed lines), and the 10 ground-level stations (in black) in the rural areas as the first station at either end of the five rail lines going through the hub station.

As a basis for benchmarking the potential representative loss of rail-operating revenues while using the baseline set of security measures, Figure 5.2 also displays specific perimeter target locations in the network where we assumed that five out of the seven potential attacks would occur. For the purposes of estimating the expected daily loss in rail-operating revenues, we defined all the attack scenarios to occur in worst-case locations (i.e., where we selected an attack on the hub-station entrance over other

[11] We calculated the ridership information on sizing comparable data extracted from WMATA for the Metrorail system, scaled down based on the lower number of 47 rail stations and 360 revenue rail cars for the notional rail system. Ridership information was extracted from FTA (2006).

[12] The revenue estimates used for the notional rail system were based on sizing comparable annual operating revenues reported for the WMATA Metrorail system based on the scaling factors used for ridership estimates. The annual operating-revenue budget and other financial data for the Metrorail system were extracted from WMATA (2006).

Figure 5.2
Notional Rail-System Network and Potential Perimeter Target Locations



RAND *MG705-5.2*

underground stations, the infrastructure supporting an elevated station closest to the city line, the external attack of a train on an elevated track closest just beyond the city line and prior to entering an underground tunnel) and a window of time during the weekday morning rush hour when the passenger density at the stations and on the trains is the highest.[13]

The economic loss in rail-operating revenue is based on estimating the expected numbers of rail passengers per day who are affected and, of those affected, the number (or percent) who cannot find alternative rail-line routes on which to commute when the notional rail system is not fully operational across any one of the five lines or 47 stations.

Table 5.10 lists the benchmark estimated loss in rail-operating revenues (in today's dollars) for each attack at and across specific perimeter target locations based on the recovery-time range estimates until operations are resumed (listed for the same cells in Table 5.8) for the notional rail system operating with the baseline set of security measures. The average loss in operating-revenue range estimates for each of the five attack modes is listed in the far right column; it represents the average of the lower- and upper-bound values for all specific target locations where the potential attack was assumed to take place divided by the total number of perimeter locations.

[13] We selected the worst case to compute the maximum loss of operating revenues over bounding the loss of operating revenues as the notional-system benchmark based on both the best-case and worst-case target locations and attack times, so we can consistently calculate each SIO's potential *maximum* rather than minimum effectiveness values at reducing the projected economic loss of rail-system operating revenues.

Table 5.10
Benchmark Loss of Operating Revenues ($ million), Estimated Across the Perimeter

Terrorist-Attack Scenario	Underground Hub Station Access	Underground Infrastructure	Ground-Level Station Entrance	Ground-Level Rail Infrastructure	External Attack on Elevated Train	Elevated Station Infrastructure	Entrances and Exits to Rail-System Operation Center Building	Entrances and Exits to Power-Plant Infrastructure	Estimated Average Loss in Rail Operating Revenues
Vehicle bombs	13–17		3–4	2–3	5–10	30–43	17–28	17–28	10.9–16.6
Small explosives	3–10		0.6–1		6.5–10		11–23	11–23	4.0–8.4
Large incendiary			0.2–0.6		3–6.5				0.4–0.9
Armed attack	0.9–1.4		0.2–0.3		1–1.7				0.3–0.4
Sabotage		0.4–0.7		0.1–0.2	0.5–0.9	0.4–0.7	1.7–2.8	1.7–2.8	0.6–1.0

Table 5.11 shows our assessment of the effectiveness of the proposed perimeter-layer SIOs capable of reducing the loss of rail-operating revenues across each of the five attack scenarios identified as high threats for the eight specific target locations within the perimeter area. For each SIO, we established a relative operating-revenue assessment rating based on the relative magnitude of reducing the rail-operating revenue loss:

- *Low reduction in operating-revenue losses* of $0.5 million or less represents a rating value of 1.
- *Moderate reduction in operating-revenue losses* between $0.5 million and $2 million represents a rating value of 2.
- *High reduction in operating-revenue losses* of $2 million or more over staying with the baseline set of security measures for the notional rail system represents a rating value of 3.

A very low reduction in operating-revenue losses is represented by a rating value of 0.5.

For each SIO, a rating value for reducing the loss of operating revenues across all five potential attack targets was computed by setting numerical values for each qualitative assessment listed (for cells across each row) using the guidelines just described, then taking the weighted average based on the total number of unique, high-risk perimeter locations (values in the top row) for the same five attack targets assessed as high risks. The overall rating value for the reduction in operating-revenue losses for each SIO is listed in the far right column of Table 5.11.

As listed in Table 5.11, adding structurally reinforced concrete pillars at equal distances between existing pillars supporting an elevated rail station (SIO 14.0) can significantly mitigate the effects of a potential terrorist car-bomb attack occurring curbside directly adjacent to an infrastructure directly underneath and supporting an elevated station. Even though this SIO may be viewed as a rather capital-intensive, large investment, depending on the number of elevated stations (such as 12 within our notional baseline system) at the perimeter level, the return in the relative improvements in effectiveness of averting fatalities (with the highest relative rating of 1.2 listed in Table 5.7) and improving recovery time (rating of 1.6 listed in Table 5.9) should be combined with the economic consequences after the attack in terms of quickly restoring operations and minimizing the potential loss of rail-system operating revenues for the number of daily commuters using this rail line (rating of 1.6 listed in Table 5.11). Given the range of potential terrorist attacks and unique number of perimeter locations within the system, this is an example of one SIO that can provide improved effectiveness from a broad damage-mitigation perspective.

Minimizing Economic Losses to Businesses. To account for the true economic impact of terrorist attacks and SIO effectiveness, it would be necessary to estimate the

Table 5.11
Assessment of Perimeter Security-Improvement Option Effectiveness in Reducing Operating-Revenue Losses

Proposed SIO	Description	Unique Types of Locations Assessed as High Risk					Reducing Operating-Revenue Loss Rating
		Vehicle Bombs (7)	Sabotage (6)	Small Explosives (5)	Armed attack (3)	Large Incendiary (2)	
2.0	Canine teams	Very low		Very low			0.3
5.0	Perimeter fencing and IDSs	Very low	Negligible	Low	Negligible		0.4
7.0	Portable (handheld) detection systems	Very low		Very low			0.3
8.0	Perimeter fencing and surveillance systems	Very low	Negligible	Low	Negligible		0.4
8.1	Tunnel surveillance system		Negligible				0.0
13.1	Fixed blast barriers	Moderate to high		Moderate		Low to moderate	1.3
13.2	Retractable bollards	Moderate to high		Moderate		Low to moderate	1.3
14.0	Structurally reinforced pillars	High		High			1.6

overall economic losses to businesses in the metropolitan area after an attack occurred. However, this would require estimating the number of rail passengers either riding or in the process of commuting to their workplaces who would be affected as well as the percentage of passengers who would not be able to use an alternative rail-line route into the city center and would instead need to find another way to commute to their workplaces (e.g., bus, private vehicle) for each working day on which the notional rail system is not fully operational on one of the five lines or 47 stations through which they would normally commute.

From an overall mass-transportation system perspective, we could compile comparable data on the total ridership of commuters using the 100 metropolitan bus routes as another option alternative. We set the average daily number of weekday bus passengers at 100,000[14] and assumed that, on average, another 100,000 commuters per day were driving into the city using private vehicles. However, to determine the viability (or likelihood) of displaced rail passengers using buses, we would have to know the average available capacity of unused seats on the buses going into the city center during the morning rush-hour commute. Furthermore, if displaced passengers were able to use private vehicles to commute into work every morning, we would have to know how many of these displaced rail passengers would carpool and, during a prolonged major shutdown of rail service (of 60 days or more), how many more vehicles could commute on the major freeways and city streets before gridlock would occur and workers would end up not going into their workplaces altogether.

Even though we estimated the total average annual gross receipts from businesses within the city at $7 billion and the total average weekday gross receipts at $25 million as the notional rail-system baseline measure representing the city's total economic income,[15] it was extremely difficult to gather the additional information needed in setting up a representative benchmark set of conditions to portray the potential overall economic loss by the businesses within the metropolitan area that were impacted for each specific attack at the same specific worst-case perimeter locations and morning rush-hour window (Figure 5.2).

Consequently, even though the logic and rating approach are the same that we used in assessing the potential reduction in the loss of rail-operating revenues, we were not able to provide a comparable benchmark table for the notional rail system using baseline security measures and another table listing the relative assessment results of

[14] The estimate of the average daily commuters using the metropolitan bus routes was based on sizing the WMATA Metrobus system ridership data extracted from FTA (2006).

[15] The annual economic index was based on assuming that 2,100 businesses were located within the city center and overall metropolitan area, with 2,000 companies having average annual gross receipts of $2 million and another 100 businesses with an average of $30 million in gross receipts. The number of companies and the breakdown of total annual gross receipts for the companies were computed and scaled down using comparable data extracted from a recent D.C. Chamber of Commerce annual business report in which gross receipts were based on data compiled from franchise board tax returns (Friedman, 2007).

the impact that implementing each relevant SIO would have on reducing the overall economic business losses caused by a terrorist attack across the different perimeter attack locations.

Combine Effectiveness Assessments with Costs

Table 5.12 lists the summarized results of the each of the four effectiveness-metric assessment-rating values for each of the SIOs capable of being effective at the perimeter level (step 3 in Figure 5.1). To get an overall effectiveness-rating value (listed in the far right column), we weighted (multiplied) the preventing-attack metric values by three and then added the three remaining mitigating-damage metric values (listed in each column) for each SIO. We weighted the preventing-attack measure to account for the fact that we had three measures of mitigation and only one of prevention.

We now add back in the annual marginal cost estimated for each of the SIOs (from Table 5.2) along with the effectiveness summary rating value (from Table 5.12) for each. Table 5.13 provides the perimeter-layer effectiveness-rating value summary and average marginal-cost estimates for each SIO.

Generate Preferred List of Security-Improvement Options at the Perimeter Layer

To generate a preferred list of SIOs at the perimeter layer, we identified a tentative order in which to implement SIOs, based on their ranked order from highest to lowest effectiveness per average marginal annual dollar (step 4 in Figure 5.1). We then reviewed the tentatively ranked list of preferred SIOs to ensure that there was a significant, cumulative, marginal improvement (net gain) in the effectiveness-rating value at the lowest cumulative, marginal cost for each SIO implemented.[16] The cost-effectiveness metric values represent a return-on-investment metric: The higher the value, the greater the relative improvement in the overall effectiveness rating per dollar estimated for procuring, installing, operating, and sustaining each option.

Table 5.14 provides the top-ranked list of preferred SIOs for the perimeter layer along with the relative effectiveness rating per average annual marginal-cost metric values for each. We then designated the top five SIOs with a metric value greater than 6.0 in the implementation order as Yes.[17] Yes SIOs should strongly be considered as preferred candidates for the perimeter layer. The remaining SIOs were placed in

[16] As a visual check to ensure that the relative slope of the cumulative-effectiveness trend or line is steeper (i.e., increases at a faster rate) than the cumulative-cost trend or line, we plotted the cumulative-effectiveness rating values (on the x axis) and the cumulative annual marginal cost (on the y axis) in the implementation order of each SIO (from left to right on the x axis). The cumulative-effectiveness-versus-cost graph for the perimeter layer is displayed as Figure B.4 in the last section of Appendix B.

[17] For this binning process, we established a nominal metric value at 6.0 or higher for a Yes decision. This value, which represents a return on investment relative to the effectiveness metric, indicates broad effectiveness across all dimensions of outcomes or very high effectiveness for a smaller number of dimensions. This value also differentiates SIOs such that a reasonable number are considered best for each security layer. The actual cutoff value used can vary from rail system to rail system, depending on the amount of passenger-security improvement budget

available and other management considerations discussed in sections later in this chapter. Because changes in this cut-off criterion could change those considered best for each security layer, they could subsequently affect the final list of recommended SIOs being considered at the system level.

Table 5.12
Perimeter-Layer Effectiveness-Assessment Summary Results

Proposed SIO	Description	Preventing-Attack Rating	Averting-Fatality Rating	Reducing Recovery Time Rating	Reducing Operating –Revenue Loss Rating	Effectiveness Rating
1.0	Enhanced security training	0.6				1.8
2.0	Canine teams	0.4	0.5	0.4	0.3	2.3
3.0	Employee background checks	0.6				1.8
4.1	Public-awareness signs and announcements					0.0
5.0	Perimeter fencing and IDSs	1.0	0.5	0.4	0.4	4.3
7.0	Portable (handheld) detection systems	0.4	0.5	0.4	0.3	2.3
8.0	Perimeter fencing and surveillance systems	1.0	0.5	0.4	0.4	4.3
8.1	Tunnel surveillance system	0.4	0.3	0.1	0.0	1.6
13.1	Fixed blast barriers	0.8	1.1	1.2	1.3	6.1
13.2	Retractable bollards	0.8	1.1	1.2	1.3	6.1
14.0	Structurally reinforced pillars		1.2	1.6	1.6	4.3

NOTE: The four effectiveness-metric rating values for the 11 SIOs listed here are the same numbers listed in tables 5.5, 5.7, 5.9, and 5.11. The total effectiveness ratings weight the prevention metric by 3 and add the three remaining metric values to account for the number of metrics used to represent prevention and mitigation. They are based on raw—as opposed to rounded—individual ratings, so they may differ slightly from the sums of the individual ratings listed. Even though all the SIOs were assessed as useful, the SIOs with blank cells were considered not to be directly able to improve those relative-effectiveness metrics we considered against threats at potential perimeter locations. Even though the option of installing public-awareness signs and increasing the frequency of public, security-related announcements (SIO 4.1) has a relative-effectiveness rating of 0.0 within the perimeter layer, it was included here because it was assessed as still being useful in terms of indirectly improving effectiveness against threats at potential perimeter locations.

Table 5.13
Perimeter-Layer Security-Improvement Option Effectiveness and Cost Summary

Proposed SIO	Description	Effectiveness Rating	Average Marginal Annual Cost ($ millions)
1.0	Enhanced security training	1.8	0.14
2.0	Canine teams	2.3	0.63
3.0	Employee background checks	1.8	0.06
4.1	Public-awareness signs and announcements	0.0	0.04
5.0	Perimeter fencing and IDSs	4.3	3.15
7.0	Portable (handheld) detection systems	2.3	0.62
8.0	Perimeter fencing and surveillance systems	4.3	4.75
8.1	Tunnel surveillance system	1.6	3.06
13.1	Fixed blast barriers	6.1	0.87
13.2	Retractable bollards	6.1	0.03
14.0	Structurally reinforced pillars	4.3	0.27

the Possible category. Possible SIOs should be considered as potential candidates in the integrated security system (discussed in a subsequent section), depending on their cost-effectiveness performance in the other security layers. The same process of computing relative effectiveness per average annual cost metric values was used for the SIOs in the other security layers, and the same basis for designating each in either a Yes or Possible category was used for each of the other layers.

The option for adding retractable bollards at the operation-control center and power-plant entrances and exits (SIO 13.2) ranks the highest in terms of the overall effectiveness rating per dollar metric value for preventing and mitigating the blast effects of a potential car bomb or large incendiary at curbsides where rail employees are entering and exiting facilities. The option with the next-highest cost-effectiveness metric is SIO 3.0, or implementing background investigations of all rail-operation and security personnel for screening out those with previous criminal records and issuing new badges to implement tighter controls in and out of restricted areas that are considered potential target locations within the perimeter layer. Following this option is the installation of structurally reinforced pillars (SIO 14.0) to elevated infrastructure supporting elevated stations and tracks. These help to mitigate damage resulting from large and small explosives. Implementing enhanced security training (SIO 1.0) for personnel and installing fixed blast barriers (SIO 13.1) curbside adjacent to station street entrances and exits complete the list of SIOs with effectiveness ratings per cost metric values at or above 6.0 at the perimeter level. The preferred list continues with possible options for consideration at the system level (i.e., SIOs 7.0, 2.0, 5.0, 8.0, 8.1, and 4.1).

Table 5.14
Preferred Security-Improvement Options for the Perimeter Layer

Proposed SIO	Description	Effectiveness Rating per Average Marginal Cost[a]	Decision[b]
13.2	Retractable bollards	193.5	Yes
3.0	Employee background checks and updated badges	30.4	Yes
14.0	Structurally reinforced pillars	16.3	Yes
1.0	Enhanced security training	13.0	Yes
13.1	Fixed blast barriers	7.0	Yes
7.0	Portable (handheld) detection systems	3.8	Possible
2.0	Canine teams	3.7	Possible
5.0	Perimeter fencing and IDSs	1.4	Possible
8.0	Perimeter fencing and surveillance systems	0.9	Possible
8.1	Tunnel surveillance system	0.5	Possible
4.1	Public-awareness signs and announcements	0.0[c]	Possible

[a] The effectiveness rating per average marginal cost value is computed as the effectiveness-rating value divided by the average annual marginal costs estimated for each SIO listed in the two right columns in Table 5.11. The proposed SIOs are listed from highest to lowest metric value, with rounding of the raw data to distinguish differences in computed values across SIOs.

[b] *Yes* indicates that the SIO is strongly cost-effective at the perimeter layer. *Possible* indicates that the SIO is potentially cost-effective at the system level.

[c] As previously mentioned, SIO 4.1 has a relative-effectiveness rating and metric value of 0.0. However, the option of installing public-awareness signs and increasing the frequency of public, security-related announcements is still included on this preferred list as a possible option for consideration at the system level, especially in improving the relative effectiveness against threats at potential rail-station target locations within the exterior and interior security layers.

Test the Robustness of the Overall Cost-Effectiveness Process

Before moving on to assessing preferred SIOs across the other layers, it is important to test the sensitivity of the assessment process and the robustness of the most preferred SIOs in terms of the set of overall effectiveness rating per average marginal cost (or per dollar) values listed in Table 5.14.[18]

Two areas of uncertainty are worth considering in assessing how robust the analytical framework and resulting values are to changes. The first is whether reducing to medium or low risk levels (e.g., based on updated results in the threat, vulnerability, and consequence analyses) for one or more of the high-risk attack modes at unique

[18] We focused the sensitivity analyses on SIO individual and relative changes across SIOs in the effectiveness-per-dollar values over changes in the Yes to Possible designations because the cutoff value of 6 for the perimeter and the other four security layers was an arbitrary setting for the purposes of illustrating this step in the assessment process.

perimeter locations would reduce the effectiveness-per-dollar values enough to change the ranking of preferred options listed in Table 5.14. We will address the sensitivity of the assessment results and changes in reducing the risk levels from specific attack modes at specific perimeter locations later in this section.

Alternatively, if the high-risk attack-mode assessments do not change, there still is the possibility that subject-matter experts (SMEs) could change their previously agreed-upon assessment of, for example, the effectiveness of installing curbside barriers to prevent or specifically deter a vehicle bomb from going off in close proximity to an entrance to an underground station, or, if the bomb is detonated, the amount of the blast that the barriers will absorb in terms of the effect on averting fatalities, reducing recovery times, or minimizing the rail-operating revenue losses before fully restoring operations to the notional rail system over the baseline set of measures.

There is a significant number of variables with likely uncertainties to consider that drive this scenario-based assessment process across the four effectiveness-outcome measures. For example, even before installing curbside barriers, terrorism SMEs would need a consensus agreement on where the likeliest effective staging location would be for detonating the vehicle bomb relative to a station entrance, which could be driven in part by the lethal effects (TNT yields) of the bomb itself and whether the objective is to cause maximum injury to passengers and others, damage to the rail infrastructure and facilities, or both. Another unbiased group of structural-engineering SMEs would then have to provide their assessments based on controlled field tests results on the effectiveness of the most relevant set of candidate contractors' barriers against the likeliest range of vehicle bombs (varying from 1,000 up to 5,000 lbs. TNT) regarding absorbing the impact from the blasts. The combined assessments from these two groups of SMEs and others could result in varying conclusions across the four effectiveness-outcome measures. Even though performing a sensitivity analysis by varying assessments for each one of the scenario-specific, high-risk attacks at a given, unique type of perimeter target location across the four outcome measures is warranted and worthwhile, we believe that the results would be very problematic and that what is most important is that the community tailoring and applying this analytical framework to an operational rail system does so based on its own experiences, characteristics, assessments, and circumstances.

As discussed, we analyzed how the effectiveness-per-dollar value results listed in Table 5.14 would change if the specific risks of the terrorist-attack scenarios changed from high to low, causing change in the assessments and the overall effectiveness ratings across the four outcome measures (preventing attacks from occurring, averting potential fatalities, reducing recovery time until operations resume, and minimizing rail-operation revenue losses after an attack takes place).

To demonstrate the robustness of the assessment process's analytical framework, we conducted a sensitivity analysis on a potential situation in which a group of terrorist specialists reassessed the threat, vulnerability, and consequences in the perimeter areas

around the facility where the rail operation-control center is located and adjacent to the power plant for our notional rail system operating with the baseline set of security measures and concluded that an attack on either of the critical infrastructures by terrorists using a vehicle bomb or a small explosive should be characterized as low- rather than high-risk incidents.

The objective of rerunning the effectiveness assessment was principally to determine the following:

- whether the total effectiveness-rating values of installing retractable bollards (SIO 13.2) would drop significantly as expected. The overall effectiveness rating for SIO 13.2 went from 6.1 (Table 5.13) to 0.8, which represents an 87 percent reduction in overall effectiveness across the four outcome measures. With the average marginal cost remaining at $0.03 million, this overall rating-value reduction is also reflected in the effectiveness-per-dollar value going from 193.5 (Table 5.14) to an 87 percent lower value of 25.1.
- how the resulting reduced effectiveness-per-dollar value for SIO 13.2 compared with the revised values for the other, more comparable infrastructure modification–based SIOs, such as installing barriers (SIO 13.1) at the other perimeter locations. First, since the risk of a vehicle bomb or small-explosive attack at a street-level location in front of one of the underground stations and the other unique perimeter locations still remains high, the overall effectiveness rating (as well as the effectiveness-per-dollar value) of installing barriers (SIO 13.1) (Table 5.13 with a value of 6.1) dropped by less than 10 percent to a 5.5 value as expected, reflecting the overall lower number of high-risk incidents going down from 23 across the unique type of perimeter locations to 19. Even though the updated overall effectiveness-rating value for installing barriers (SIO 13.1) of 5.5 is now almost seven times higher than the comparable rating value for installing bollards (SIO 13.2) of 0.8, the updated effectiveness-per-dollar value for installing bollards (SIO 13.2) of 25.1 is still almost four times higher than the updated effectiveness-per-dollar value of 6.3 for installing barriers (SIO 13.1). The comparison of these two SIOs is as expected. Even though there is less of a compelling need for bollards as a perimeter-layer security measure against these two attack modes at these two unique perimeter locations, this option still has the potential to provide more effectiveness per dollar than installing barriers, driven by the average marginal costs for installing barriers (SIO 13.1) being almost 28 times more expensive for our notional rail system than the comparable cost for installing bollards (SIO 13.2) at $0.03 million (Table 5.13).

In the last section of this chapter, we also discuss the potential up-front factors to consider and collective set of information to gather in tailoring the analytical framework to assessing a more complex rail system than our notional system.

Assess Security-Improvement Options Across All Layers and Generate System-Level Recommendations

After applying the same approach of steps 1 through 4 for the other four security layers, we summarize all the effectiveness assessments in Table 5.15, which shows the results for the other layers alongside the same results for the perimeter layer previously shown in Table 5.14 (step 5 in Figure 5.1).

Within each security layer, there are three to five preferred SIOs (Yes rankings). Several other SIOs are in the Possible category, which should be considered from a system-level assessment perspective, depending on their interdependence at improving security in one of the other layers or included as part of the recommendations on the basis of being low cost and affordable in the near term to implement. This analysis makes clear that an SIO may be preferred for one security layer but not for another. It also illustrates that some SIOs are preferred for more security layers than others.

The preceding sections have identified a set of preferred SIOs for each of the system layers. Table 5.15, for example, implies that a security planner should start with enhanced security training, because such training is highly cost-effective in all five layers. Table 5.15, however, does not take into account practical realities of affordability concerns such as annual budget (cost) limits and the sometimes long-term nature of planning for security improvements to fit within plans for other rail-system capital and modernization improvement–related expenditures.

Table 5.16 presents the same information as Table 5.15 does but organized in a different fashion that incorporates some of the real-world affordability cost constraints that planners might encounter. It differentiates SIOs based on their highest to lowest cost-effectiveness (effectiveness per marginal cost dollar) ranking and their least expensive (lowest) to most expensive (highest) average marginal annual costs, thereby creating a portfolio of recommendations divided into four categories for the notional rail system.[19]

The list of system-level recommendations in Table 5.16 is just one of many ways in which a security portfolio could be constructed based on the cost-effectiveness analysis. For example, similar portfolios could be developed to organize preferred security measures by potential ease and speed of implementation (which may correlate inversely with cost), by dependency or logical sequential ordering of SIOs, or to reduce risk at particular locations or of particular attack modes. As an illustration, an

[19] We derived this particular illustration by categorizing the SIOs based on low (less than $0.7 million) and high (more than $0.7 million) cost. We then created a composite ranking for each SIO, based on summing the layer-level cost-effectiveness designations (1 for yes and 0.5 for possible) to rank them within the broader inexpensive and expensive categories, thereby creating the four categories and results shown in Table 5.16. This approach favors SIOs that illustrate broad effectiveness across layers over SIOs that may be highly cost-effective but for only a single layer. Another alternative, if a security planner wished to consider SIOs that are extremely cost-effective even if for a single layer, would be to categorize SIOs into cost categories based on a raw, total cost-effectiveness measure. Such decisions for creating a portfolio of options are best made at the system level based on the operational context, circumstances, and priorities.

Table 5.15
Preferred Security-Improvement Options Across Five Security Layers

Proposed SIO	Description	Perimeter	Exterior	Interior	Restricted Areas	Rail Vehicles
1.0	Enhanced security training	Yes	Yes	Yes	Yes	Yes
2.0	Canine teams	Possible	Possible	Possible		Yes
3.0	Employee background checks and updated badges	Yes			Yes	
4.1	Public-awareness signs and announcements	Possible	Yes	Yes		Possible
4.2	Rail-status LED displays		Possible	Possible		Possible
5.0	Perimeter fencing and IDSs	Possible			Possible	
6.0	Passenger- and baggage-screening systems		Possible			
7.0	Portable (handheld) detection systems	Possible	Yes	Yes		Yes
8.0	Perimeter fencing and surveillance systems	Possible			Possible	
8.1	Tunnel surveillance system	Possible				
9.0	Rail-vehicle surveillance systems					Possible
10.0	Personnel ACSs				Possible	
11.0	Hybrid security system		Possible	Possible		
12.0	Blast-resistant containers		Yes	Yes	Yes	
13.1	Fixed blast barriers	Yes	Possible	Possible		
13.2	Retractable bollards	Yes			Yes	
14.0	Structurally reinforced pillars	Yes	Possible	Possible		

NOTE: *Yes* indicates that the SIO is strongly cost-effective for a specific security layer. *Possible* indicates that the SIO is potentially cost-effective at the system level.

argument can be made to implement enhanced security training first because it is also a prerequisite for deploying rapid-response teams to effectively use portable (handheld) detection devices that can be deployed alongside canine teams. Security planners could also consider the interdependence of risk and SIOs across layers. For instance, they could qualitatively assess the impact that a particular SIO implemented in one security layer may have in shifting risk in subsequent layers, which, in turn, could influence the risk and preferred SIOs in these layers.

Table 5.16
System-Level Security-Improvement Recommendations

Responses	Security-Improvement Recommendations	Average Marginal Annual Cost ($ millions)
Inexpensive solutions with highest cost-effectiveness payoffs	Implement enhanced security training (SIO 1.0)	0.14
	Use portable (handheld) detection systems (SIO 7.0)	0.62
	Increase number of signs and public-address announcements (SIO 4.1)	0.04
	Install blast-resistant containers (SIO 12.0)	0.21
	Add canine team (SIO 2.0)	0.63
Inexpensive solutions with reasonable cost-effectiveness payoffs	Install retractable bollards (SIO 13.2)	0.03
	Institute employee background checks and issue updated badges (SIO 3.0)	0.06
	Install structurally reinforced pillars (SIO 14.0)	0.27
	Install rail-information status displays (SIO 4.2)	0.22
More expensive solutions with highest cost-effectiveness payoffs	Install fixed blast barriers (SIO 13.1)	0.87
	Install perimeter fencing and IDSs (SIO 5.0)	3.1
	Install perimeter fencing and perimeter surveillance systems (SIO 8.0)	4.75
	Implement hybrid security system (SIO 11.0)	8.30
Expensive, longer-term solutions for future consideration	Add rail-vehicle surveillance systems (SIO 9.0)	1.35
	Upgrade personnel ACSs (SIO 10.0)	1.40
	Install passenger- and baggage-screening systems (SIO 6.0)	1.75
	Install tunnel surveillance system (SIO 8.1)	3.06

Before generating an integrated system-security implementation plan, security planners should prioritize the list of recommended SIOs based on a logical order of implementation. Prioritization of the list of recommended SIOs could occur through

contextualizing the implementation of SIOs based on practical considerations (e.g., operations, resources, specific security concerns) by shifting the ranking of SIOs through a qualitative or quantitative process developed by security planners in each individual rail system.

These options are just a few of many ways in which a final, system-level list of recommended SIOs could be determined. The remaining sections in this chapter discuss the economic, budgetary, and other factors that could be considered in producing an integrated system-security implementation plan that is relevant not only for our notional system but for all rail systems.

Deal with Economic and Budgetary Limitations

Rail operators and security managers will have to generate an implementation schedule based on operational dates for when security improvements are needed in the near, mid, and far terms to close security gaps and put in a common-sense sequence of actions that can be time-phased with a roll-up of the annual budgets needed.

In many cases, inexpensive SIOs with the highest payoffs in terms of overall relative improvements in effectiveness tend to be on the top of the list to be implemented first. However, the estimated investment and recurring costs of time-phasing and integrating new measures into a rail system to close security gaps will have to fit from an affordability perspective within the different and fluctuating economic conditions and budgetary limitations of all the stakeholders with vested interests in the rail system. Therefore, the decisionmaker should have the ability and assessment tools needed to readjust priorities and alter the sequence for implementing a set of SIOs as changes in economic conditions and annual budgets occur. As needed, trade-offs across different SIOs may have to be made in terms of start dates to fit within these annual fiscal constraints.

In addition, in the case of procuring, for example, fixed barriers at curbside passageways to rail stations, large quantity-buy discounts and other economy-of-scale decisions may have to be considered for balancing the budgetary constraints to fit within the overall goals and objectives of the rail system's strategic and tactical security plans.

Recognize Interdependence Across Security Options

As alluded to in our previous discussions of SIO assessments for the notional rail system, any security alternative being proposed or assessed has an interdependent relationship with an existing baseline or other proposed set of security measures, besides those SIOs within a multilayered security system. The term *interdependent* is used to mean a necessary and sufficient set of assets (e.g., a person in the loop, communication-network infrastructure) is either in place or required to get the full return on any one specific SIO. Also, besides an effective communication network, a clear set of organizational roles and responsibilities should be established along with

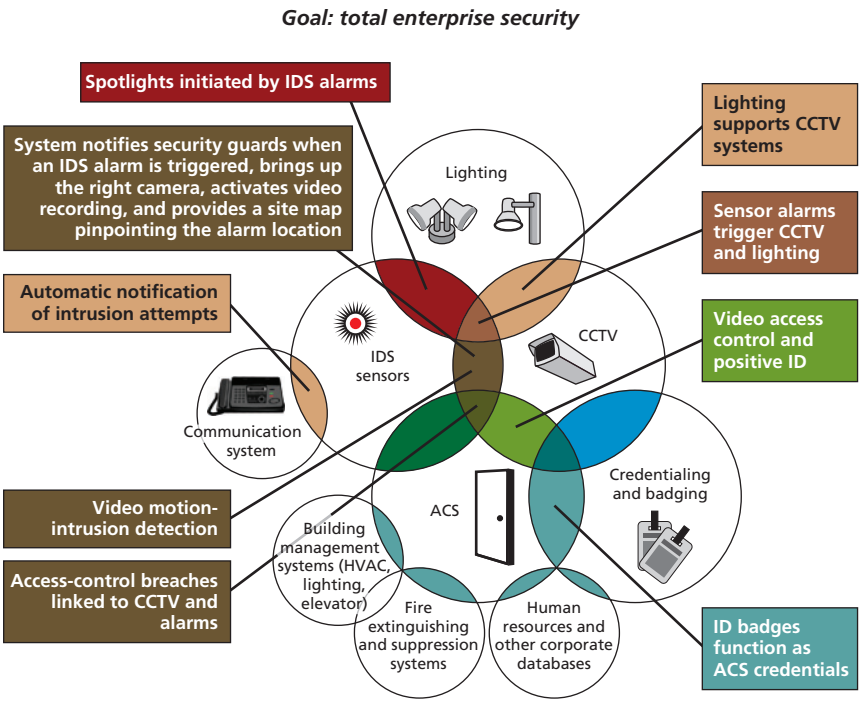
proper training and operational protocols within and among the rail operators, security officers, rapid-response teams, and emergency responders using the network.

For example, the effective use of CCTV cameras as part of a video surveillance system requires a sufficient number of monitors and adequately trained 24/7 staffing to detect video images of passengers' suspicious behavior and to alert and deploy the most effective rapid-response security team directly to the specific location where the incident took place.

As another example of the interdependence across SIOs, Figure 5.3 displays security assets that need to be in place and operate with a personnel ACS within a rail system.

If perimeter fencing along with an IDS is used or proposed within a secured or restricted area of the station and an alarm goes off, the system's effectiveness in detecting a potential terrorist is directly affected by its ability to automatically, or with security-control personnel available in the loop, activate increased lighting within that area or turn on CCTV cameras (or both), and alert a rapid-response team of security personnel to quickly deploy to where the IDS alarm went off.

Figure 5.3
Example of Interdependence of Security Measures for Access-Control Systems



SOURCE: Adapted from Rabkin et al. (2004).

RAND *MG705-5.3*

One of the lessons learned through WMATA Program of Response Options and Technology Enhancements for Chemical/Biological Terrorism (PROTECT) demonstrations was that, in addition to reducing false alarms, training for rail-operation and transit-security personnel was needed to effectively respond on site to a chemical incident (CUTR, undated). Furthermore, when using chemical-detection systems, the study authors discovered that improved lighting and higher-quality CCTV cameras for surveillance were needed to replace old cameras that had degraded over time. Also, the new CCTV cameras need to have pan, tilt, and zoom features that can be controlled remotely from the operation-control center, not just from a station kiosk. Cameras also require recording capability and improved radio reception to ensure that there are no dead spots in all areas of the station and lower-level platforms. Finally, hazmat teams need to be coordinated to prognosticate and validate prediction of hazard-zone areas and to communicate important information to emergency responders as quickly as possible.

Ensure a Proper Balance of Security-Improvement Options

One of the considerations in selecting the most optimal cost-effectiveness assessment mix of SIOs is the concern that some terrorist acts will likely still succeed. Given the relatively large number of potential antiterrorist security measures that can be implemented and faced with the impossibility of omnipresent protection, difficult system-level issues and trade-offs arise, especially when balancing the level of "acceptable losses" by selecting the mix of security measures focused on improvements in deterrence and detection (countermeasures) alternatives versus those focused on improving protection (i.e., infrastructure and facility hardening), emergency responses, and recovery-related initiatives.

Thus, decisionmakers should review the list of SIOs recommended across the four categories represented in Table 5.16 to ensure that there is a proper balance of measures in place. For example, use of canine teams, in addition to detecting explosive particles on passengers and their packages, provides a potentially higher level of deterrence value than other measures might and sends a positive message to the passenger community that rail security is proactively watching over them. Furthermore, installing perimeter, station, tunnel, and rail-vehicle surveillance systems is used to detect a potential terrorist attack. However, if any one of the surveillance systems is still functioning effectively after a terrorist attack, it can also benefit the emergency-response teams in helping to direct an appropriate set of actions to remediate the effects of a chemical threat or provide video images in helping the team in the location, search, and rescue of trapped passengers and others within different locations of the rail system.

Assess Timelines for Implementing Security-Improvement Options

In finalizing the security implementation plan, the timelines for closing the security gaps are critical in establishing the need dates and determining when a rail-system

agency should implement its recommended system-level SIOs. Accommodations should be made to accelerate the implementation of countermeasures or drop other security measures if there are projected shifts in the type or form of potential terrorist attacks (e.g., the increased training in detecting and preventing terrorist attacks using IEDs).

In addition to establishing need dates for closing security gaps and establishing an implementation timeline, specific security countermeasures, such as portable (handheld) detection systems, should be considered only after completely assessing the technical maturity level of the product and the TRL of development to identify when it will be fully matured, field-tested, and operationally available. The more field data that exist, the more confidence decisionmakers will have in the system's expected performance and reliability, as well as in the projected annual recurring cost of maintaining these systems.

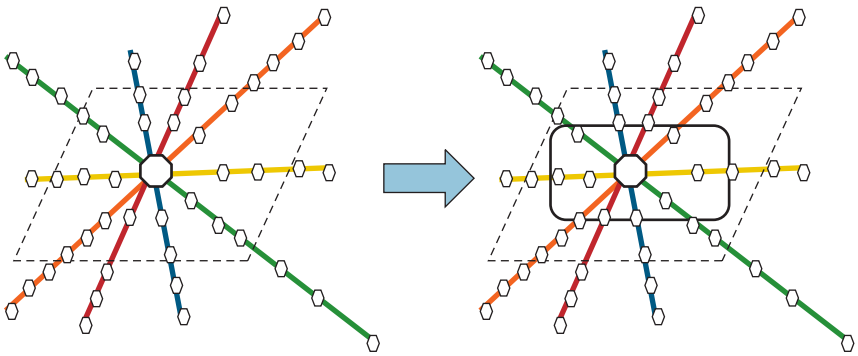
Furthermore, before time-phasing or incrementally implementing a list of recommended SIOs, other system-level trades should be performed to consider the current and possible changes in the density of passengers moving through stations and onto trains as portions of the populace move out to suburbs or the city's center of business and commerce is projected to shift and become more decentralized. Considerations about when to implement SIOs should also factor in any major changes to the rail system as part of the broader regional transportation plans and proposed investments, especially in responding to any expected increases in the volume of passengers relying on the system.

Limitations on Using the Analytical Assessment Process

In closing, we want to point out that, even though this assessment process provides an analytical framework for evaluating and ranking the overall relative effectiveness of proposed SIOs over the baseline security system, the accuracy of being able to project reductions in the probability of preventing a terrorist attack from occurring, the number of reduced fatalities averted, the expected reduction in recovery times, and minimizing operating-revenue losses after the attack takes place can vary based on best assessments of false-alarm rates of detection systems to lethality assessments of the reduced blast-radius impacts of infrastructure- and facility-hardening measures, scenario-based simulations, and the best judgments of SMEs.

Finally, we recommend that the analytical assessment approach we described be tailored or customized to each rail system for operation management and security officers' joint use. To provide a sample of the major considerations involved in adapting the assessment approach, we reintroduce the notional rail system (the left panel) and present a more complex rail-system network (the right panel) in Figure 5.4.

Figure 5.4
The Notional Passenger-Rail System and Potential Changes to It



RAND *MG705-5.4*

Going from a single, central hub to multiple hubs and transfer points at which passengers have several options in going from station A to station B adds complexity, because the number of potential terrorist-target locations may increase and the likelihood of multiple, simultaneous attacks occurring at several locations may also increase over the notional baseline system.

Even though the unique type of rail locations mapped across the security layers may not change, the threat and vulnerability risk-assessment levels used as the basis for determining the usefulness of options across each layer may change, and the prioritized ranking of the SIOs may be quite different from that in the notional baseline system.

Since peak passenger densities during morning and afternoon rush hours will probably shift from a central hub to one or more transfer-point stations, the effectiveness-assessment metrics of the changing number of potential passenger fatalities averted and the impact on the length of the recovery time until operations can be restored for a given terrorist-attack scenario will have to be reevaluated, especially in potentially rebuilding stations with multiple platforms. In addition, the same reassessment of the economic consequences will be necessary as the ability to reduce rail-operating revenue losses for a specific SIO over the current baseline set of security measures for this more complex rail system will be dramatically different from that of the notional baseline system.

Furthermore, the disruptive effects of a terrorist attack on closing down operations can be quite different within this more complex rail network across the different stations and rail lines within the system, especially in cases in which all or a portion of some lines have no redundant rail tracks and others do, which, after an attack occurs, can affect displaced passengers' ability to find alternative lines on which to commute to work.

Therefore, the final projected percentage value of expected lost operating revenues (and the overall economic impacts on the business community) depends on the following:

- how the rail network is configured, as we described previously for the hub-spoke or more complex configurations
- the number and percent of the total daily passengers affected by a terrorist attack
- the alternative modes of transportation of buses, taxis, and private vehicles available for their commute into the center of the city until all lines of the rail system are fully operational.

CHAPTER SIX

Rail-Security Policy Considerations

Given the open and accessible characteristics of rail systems, the unpredictability of terrorist attacks, the continual evolution of risk as terrorists learn and improve on their capabilities, and finite resources for security provisions, the United States faces a complex security problem that has existed for decades. This book has illustrated a process—a framework and a broad range of management considerations—for thinking through how to systematically improve the security of U.S. passenger-rail systems to help ensure maximum protection at the lowest cost.

In this chapter, we step back from the detailed analysis of protecting the notional rail system to highlight some key lessons for security planners and policymakers. We begin with lessons that may be helpful at the rail-system level, lessons aimed mostly at rail-system operators and at those responsible for security decisionmaking at the local level. We then turn to discussing the future of rail security and the trade-off between providing rail security and the security of everything else.

Rail-Security Lessons at the System Level

To ensure maximum security for a given amount of resources, those responsible for leading security efforts for specific rail systems should consider adopting and conducting analytical processes such as those described here for shaping security decisions. Any such framework should, of course, be tailored to each rail system for operation management and security officers' joint use, because the disruptive effects of a terrorist attack can be different across and even within rail systems.

Security planners can draw from the framework and analysis described here to assess and structure their SIOs. The first step in any such analysis, which many system administrators have already done, is to conduct a detailed vulnerability assessment of the rail system. Drawing from our analysis, this can be accomplished by determining which scenarios should be used in assessing a particular rail system's vulnerabilities. The threat of these forms of attacks can then be assessed relative to potential vulnerabilities that exist in each of the five layers of security differentiated here—perimeter, exterior, interior, restricted areas, and rail-car assets. Officials can then plan

for improving security relative to increasing SIOs at the most vulnerable locations across the layers and throughout the entire system.

Our analysis provides the relative cost and effectiveness for many currently available and tested SIOs known to us at the time of this writing. Drawing from their specifically conducted vulnerability assessments, security planners can then compare SIOs for each vulnerability relative to their costs and overall utility. This can help them to decide how to most cost-effectively spend a fixed amount of security-improvement dollars or estimate the amount of resources they require to most effectively limit the risk to specific vulnerabilities.

As we did in our analysis of the notional rail system, system planners should assess such SIOs at the margin. No rail system begins from a blank slate when it comes to protective efforts; even at a minimum, the system's proximity to and coordination with local response resources provides a baseline level of some protection. As a result, questions of cost-effectiveness of security investments cannot be rigorously assessed without considering what is already in place. Thus, rigorous assessment of the relative effectiveness of a security-improvement investment is context-specific.

It is also the case that the cost-effectiveness assessment in this study focused on measures designed to detect and prevent attacks on rail systems and to mitigate the damage from those that occur. In considering the terrorism risk that these systems face, planners have a much wider range of choices available to them in addition to traditional security countermeasures. These include planning for effective response to an attack if and when one does occur (also potentially limiting the damage that terrorists can cause even if they successfully carry out an operation) and preparing to recover quickly from an attack to reduce the economic and other impacts of an attack. Actively managing risk can also result in planning effective responses that do not overreact to false incidents, hoaxes, and actual attacks, which otherwise could lead to more disruption than necessary. For example, creating procedures to quickly assess the danger posed by unattended items (as some rail systems have) can prevent unnecessary delays and improve rider confidence in rail security. While preventing attacks before they occur would clearly be preferred, it is important to consider the contribution made by security and preparedness measures across the full spectrum of options in crafting a strategy to harden rail systems against terrorism.

Although the focus of this book and of the analysis underlying it is to protect rail systems from terrorist attacks, protective investments may have other benefits as well. For example, most rail systems have some incidence of criminal activity, including violent crime, and other safety concerns as well (Federal Transit Administration Office of Safety and Security, and John A. Volpe National Transportation Systems Center, 2004). Thus, measures that protect the rail system against terrorism (e.g., improved response capabilities, evacuation routes) may also be useful in addressing other risks. Security planners could consider estimating these crossover benefits when they are deciding on SIOs, particularly when two SIOs have similar risk-reduction benefits.

Because defensive measures against terrorism seek, by definition, to counter the efforts of strategic actors, those in charge of acquiring SIOs must consider how terrorist groups might react to potential security-improvement defenses put in place, so that they can make more informed investment decisions. If a given SIO is visible to the general public, as well as to terrorists, and there are simple ways to circumvent or overcome this SIO, it cannot be cost-effective if it only displaces (e.g., by time or location within the rail system) the attack rather than reducing the probability of an attack (Jackson, Chalk, et al., 2007). However, if the SIO's presence is enough to suggest that the rail system is too hardened for an attack, thereby reducing the probability of attack, it can be an effective deterrent (though possibly displacing the attack to more vulnerable targets). In the future, the progress of more covert forms of protective security measures (e.g., passive millimeter wave [MMW] techniques integrated into surveillance CCTV cameras) may be more viable options worth considering as a mid- to long-term solution.

Beyond simply determining whether there are ways to defeat particular defenses, security planners should also consider whether an adversary can undermine in other ways the advantage that an SIO provides. Detection technologies provide a useful example. If a detection system is set up with the understanding that a tolerable level of false alarms is one per month and a terrorist group has the knowledge and capability to devise a way to cause what appear to be false alarms at a much higher rate, the terrorist group can significantly reduce the value of the detector's expected level of performance. Furthermore, if responding to each alarm has a significant operational cost (e.g., evacuating a station, shutting down part of the system), the ability to cause false alarms actually becomes something that gives considerable leverage to the terrorist, by turning a relatively useful SIO that was otherwise a defensive asset into a liability. Acquisition leadership and security planners have to understand or have SMEs with the technical knowledge available to fully evaluate, field test, and troubleshoot the realized versus proposed performance of vendor's latest detection devices and thoroughly determine their real usefulness in the operational rail environment to which the equipment will be exposed before any smart investment decisions are even considered.

The Future of Rail Security

Many factors affect the long-term utility of the framework used in this analysis. Indeed, the interaction between terrorists and security is a dynamic one in which both sides of the equation attempt to gain the upper hand. We know from observation and analysis that terrorists study our security measures, systematically probe them in certain circumstances, and attempt to develop countermeasures that will defeat, disable, or

otherwise render neutral our security measures.[1] How much of the dynamism can we predict and what are the consequences for rail security?

We have already witnessed some important changes in terrorist-attack patterns against transportation in the few years since 9/11. Notable examples include the terrorists' clear efforts to develop bombs that defeat our detection capabilities, such as Richard Reid's attempt to detonate a shoe bomb and terrorist efforts to develop liquid bombs. Although we can predict with near certainty that terrorist-attack patterns will change, it is far more difficult to predict with any certainty how they will change. Will they shift to unconventional weapons as a way of circumventing defenses that are oriented largely toward thwarting conventional attack methods?

Thus, a key objective of designing a system for rail security is that the measures should not be static. Security assessments themselves must be periodically updated and refreshed to ensure that security measures are appropriate to the threat as it is currently being manifested. Likewise, attack patterns must be reviewed at regular intervals to ensure that the security portfolios deployed remain robust to any changes in the attack pattern. Security professionals should be particularly alert—through security trade associations, contact with intelligence officials, and other resources—for specific evidence that terrorists are adapting their behavior to circumvent security measures.

Another key element of developing and maintaining robust security measures is investment in research and development. Technology can undoubtedly play a role in diminishing the terrorists' ability to attack successfully. Improvements in technology can similarly reduce the indirect costs of security: the time required to screen individuals or areas to detect threats, the consequences of false alarms triggering security or response action, and the need for invasive security measures, such as hand searching. Combinations of technologies can help compensate for the limitations or vulnerabilities of individual security measures; for example, the combination of surveillance with fencing to protect system perimeters can help make it more difficult for an attacker to simply cut through a fence to get inside. However, because technologies are often crafted to address individual threats and based on particular assumptions about the threat environment, security planners must be vigilant for changes and, if possible, stay ahead of changes that potential attackers make. If we simply assume that a given set of security measures will provide protection indefinitely, security planners will be left to scramble to respond to the nearly inevitable changes in the threat.

An investment in human capital is needed as well. Acknowledging the importance of technology, case-study respondents echoed that there is no substitute for the human element. Though technologies can perform many security functions, the people who use and monitor them are frequently the most critical element of the overall security system. Although increasing computing power is being integrated into security

[1] For a detailed examination of terrorists' efforts to counter security measures, see Jackson, Chalk, et al. (2007).

devices, there is no substitute for a person who can quickly validate and evaluate the information provided by detection, monitoring, and other technologies and make a decision about what rapid-response deployment actions to communicate and implement to address a potential threat. As a result, investments in the training of system staff, coupled with programs to test those skills and ensure that personnel remain vigilant even if no incidents have occurred for some time, are essential complements to physical security measures.

Finally, terrorists' efforts to defeat or circumvent technologies can be incorporated into security modeling through a number of mechanisms, such as decreasing the assumed effectiveness of security measures over time (to simulate terrorist learning or adaptation to security) or increasing the costs associated with fielding the security measure (to simulate the need for continued investment to stay ahead of the terrorists). Ultimately, the decision about investing in technology and policies and procedures to protect a critical asset such as passenger rail is a difficult one. Investment decisions are best when they are made not in the face of crisis but instead through deliberative processes that weigh the costs and effectiveness of various approaches to security. Investment decisions should be made not only based on the knowledge at hand but with an attempt to understand how adaptable the security assets are at handling changing problems in the future.

Rail Security Versus the Security of Everything Else

This book demonstrates the value of an analytical framework for informing and guiding strategic decisionmaking for improving passenger-rail security. National policymakers must recognize that the security of any one rail system is not necessarily independent of the security of other rail systems or other targets more generally. A common response by terrorists to the deployment of security measures is simply to move attack operations away from the defended area to softer targets located elsewhere. If defenses are deployed in one rail system, this behavior could move risk from one site to another. Likewise, if rail-security measures are increased across the entire rail-transportation system, attacks may simply be displaced onto other targets, such as a shopping mall or sport stadium. Under some circumstances, displacement could be viewed as a favorable outcome, if, for example, the attack were displaced to a location that is much easier to respond to than the original target location would have been.

Given that security in one setting relates to security in another, federal policymakers ultimately must decide how best to allocate security dollars not only across rail systems but also across other modes of transportation, critical infrastructure, and public venues. We cannot, from this analysis, draw conclusions about whether authorities should spend more on rail- and less on air-transportation security because we did not conduct such cross-mode and cross-target comparisons. We can, however, point to

the applicability of this assessment methodology to decisionmaking about allocating security resources generally. We strongly encourage analysts, scholars, and researchers to extend the application of this form of methodology to such critical resource-allocation problems.

Conclusions

It bears repeating that the prioritized SIOs identified in this book are specific to the notional system we analyzed. Furthermore, the analysis performed here captures a point in time—the attractiveness of different SIOs in our prioritization is driven by the current costs for those options and their current perceived effectiveness. Over time, both of these factors are likely to change as costs come down for some options and additional data become available on the benefits that different technologies and protective measures provide. As a result, even if the preferred SIOs described here are viewed as reasonable for a given system, that conclusion is perishable. As costs change and the effectiveness of different options against threats of concern becomes clearer, the options will need to be revisited to assess any necessary shifts in priority.

These limitations notwithstanding, the methodology presented here is useful for planning rail SIOs. A logical next step with this methodology is to test it on additional rail systems that operate with configurations of differing complexity. The purpose of such experimentation would be twofold. First, we would like to learn from additional applications of the methodology whether there is a finite number of system configurations with which we need to concern ourselves. Put another way, it is possible that the same set of preferred options will consistently emerge, regardless of system complexity, or that similar sets of preferred options will emerge for different clusters of system complexity. Since both risk and the nature of preexisting security measures will vary by the type of system examined, such experimentation will also give some insight into the dynamic nature of the threat- and security-assessment processes and, perhaps, the timeline over which the assessments need to be repeated to counter the fact that terrorists wield new methods and learn their targets' defenses over time.

Second, the methodology should be tried on systems of differing complexity to better understand the information-gathering burden it poses. The methodology is most useful if the baseline set of operational and security-related information it requires is relatively easily obtained in a consistent and comprehensive manner. To some extent, our notional model is a hybrid that embodies features of multiple rail systems. We know relatively little about how much of the information needed to use this methodology an individual rail system will have readily at hand.

Even without conducting these additional tests, we have demonstrated that the issue of improving rail security can be analyzed in cost-effectiveness terms using a rela-

tively simple methodology. The challenge now is to further refine the methodology and transform it into a tool that is accessible to security planners.

APPENDIX A

Qualitative Risk Assessment of Rail-Attack Scenarios

In Chapter Three, we presented the results of our qualitative risk assessment of rail targets. In this appendix, we briefly present more detail on how the risk assessment was conducted.

The scale of terrorism risk is driven by the combination of *threat*, system *vulnerability*, and the potential to produce *consequences* as a result of specific attacks. Detailed assessment of terrorism risk for the selection of security measures would ideally be performed at the level of the individual rail system, since differences in design and current security levels will determine how a given attack scenario would affect the system.

In the absence of such system-specific information, we have performed a qualitative comparison of different attack modes staged against component targets within a notional rail system and assessed the consequences produced in similar past attacks to produce a generalized risk ranking to guide our discussion of security measures. For each element of risk, data from past terrorist activities and qualitative vulnerability information were used to rank risks using a basic scale of high, medium, and low levels.[1]

Threat

Threat is created when an adversary has both the intent and capability to stage a particular attack against a rail target. For our analysis, we examined eight attack modes:

- large explosive (e.g., vehicle bomb)
- small explosive (e.g., emplaced bomb or carried suicide device)
- large incendiary (e.g., vehicle containing flammable material)
- small incendiary
- armed attack
- unconventional weapon
- sabotage

[1] See Willis et al. (2005) and Greenberg et al. (2006) for a broader discussion of terrorism-risk analysis and an example of a previous qualitative terrorism-risk ranking effort.

- hoax attacks or threats.

Data on past terrorist use of these attack modes against rail targets were used to categorize the attacks into high, medium, and low threat classes (analysis of rail incident data compiled from National Memorial Institute for the Prevention of Terrorism and RAND Corporation, ongoing; Jenkins, 1997, 2001; Rabkin et al., 2004; and Monterey Institute of International Studies, undated[b]). Based on the data reported in Tables 2.1 and 2.2 in Chapter Two, attacks were categorized as high threat if they were used in more than 20 percent of attacks, medium threat if they were used in between 5 and 20 percent of attacks, and low threat if they were used in less than 5 percent of attacks. Because our data do not include comprehensive information on the size of incendiaries or explosives used, the cases of large explosive and large incendiary were demoted one threat level from their small counterparts to reflect their greater logistical burden for an attacker. This produced a threat ranking for the attack modes, as shown in Table A.1.[2]

Since threat is most correctly associated with the intent to use a weapon at a particular location in a rail system (an attack scenario), we also used the distribution of past attacks on rail targets to estimate an aggregate threat measure. The distribution of attacks shown in Figure 2.1 in Chapter Two shows that past attacks fall into two broad groups: more common attack locations (stations, inside train cars, outside but targeting train cars, and tracks) each making up between one-sixth and one-quarter of all attacks and much less common attack locations (supporting infrastructure, equipment alone, and areas outside stations) each making up less than one-twentieth of

Table A.1
Threat Ranking of Attack Modes

Attack Mode	Threat Ranking
Large explosive	Medium
Small explosive	High
Large incendiary	Low
Small incendiary	Medium
Armed attack	Medium
Unconventional weapon	Low
Sabotage	Medium
Hoax attacks or threats	Medium

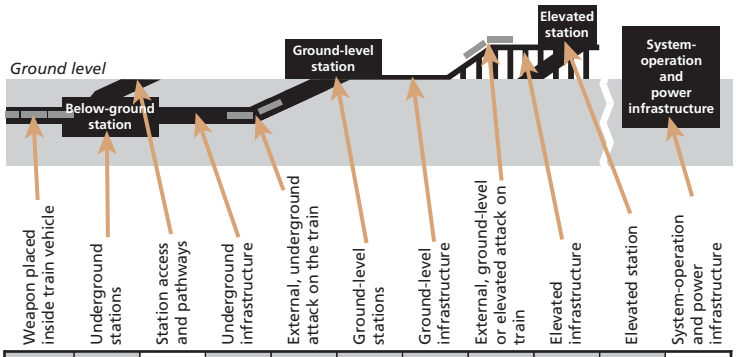
[2] This assessment of terrorist-threat levels is explicitly based on past terrorist behavior, and significant changes in future tactical choices would affect the conclusions of this assessment.

attacks. As a result, to produce an aggregate threat value for specific attack scenarios, the threat estimated for a given attack mode (Table A.1) was adjusted downward by one category for attack locations that were only rarely the site of attack (i.e., fell into the less common attack location group). The result of this threat assessment of scenarios is shown in Figure A.1.

Vulnerability

Accurate judgments about specific vulnerabilities to given attacks depend on the design and security at a particular rail system. To support the qualitative assessment for this work, we have graded vulnerability based on a judgment on the practicality of a given attack mode at a site in the notional rail system discussed in the text. For example, although a large, vehicle-sized bomb could be readily used to attack passengers at station access and pathways (areas accessible to vehicles that could carry such a device), it would be exceedingly difficult to use such a large bomb in an attack on an

Figure A.1
Qualitative Threat of Specific Rail-System Attack Scenarios

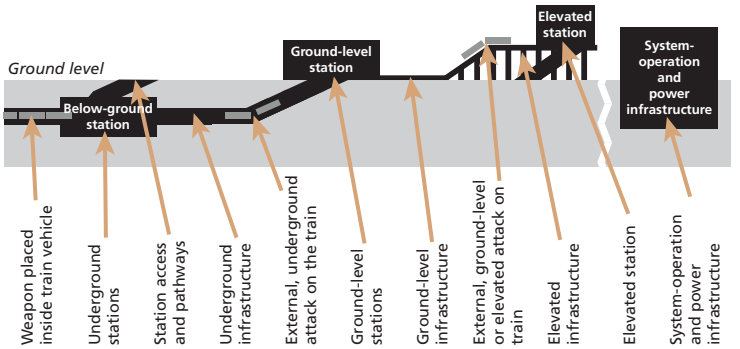


	Weapon placed inside train vehicle	Underground stations	Station access and pathways	Underground infrastructure	External, underground attack on the train	Ground-level stations	Ground-level infrastructure	External, ground-level or elevated attack on train	Elevated infrastructure	Elevated station	System-operation and power infrastructure
Large explosive	Medium	Medium	Low	Medium	Medium	Medium	Medium	Medium	Medium	Medium	Low
Small explosive	High	High	Medium	High	High	High	High	High	High	High	Medium
Large incendiary	Low	Low	Low	Low	Low	Low	Low	Low	Low	Low	Low
Small incendiary	Medium	Medium	Low	Medium	Medium	Medium	Medium	Medium	Medium	Medium	Low
Armed attack	Medium	Medium	Low	Medium	Medium	Medium	Medium	Medium	Medium	Medium	Low
Unconventional weapon	Low	Low	Low	Low	Low	Low	Low	Low	Low	Low	Low
Sabotage	Medium	Medium	Low	Medium	Medium	Medium	Medium	Medium	Medium	Medium	Low
Hoax or threat	Medium	Medium	Low	Medium	Medium	Medium	Medium	Medium	Medium	Medium	Low

RAND *MG705-A.1*

underground component of a rail system.[3] Similarly, the use of an unconventional weapon is likeliest to be effective in fully enclosed areas of a system (e.g., inside trains), could be used (but perhaps less effectively) inside a station above ground, and would be least effective in open-air areas. Attack modes that were judged most impractical at a given site were coded low, those viewed as well matched to the site were coded high, and cases that fell between those two extremes were coded medium. Vulnerability to each attack mode is summarized in Figure A.2, in which combinations coded high are shown in black, those coded medium are shown in gray, and those coded low are shown in white.

Figure A.2
Qualitative Vulnerability of Rail-System Components to Specific Attack Scenarios



	Weapon placed inside train vehicle	Underground stations	Station access and pathways	Underground infrastructure	External, underground attack on the train	Ground-level stations	Ground-level infrastructure	External, ground-level or elevated attack on train	Elevated infrastructure	Elevated station	System-operation and power infrastructure
Large explosive	Low	Low	High	Low	Low	High	High	High	High	High	High
Small explosive	High	High	High	Medium	High	High	Medium	High	Medium	High	High
Large incendiary	Low	Low	High	Low	Low	High	Medium	High	Medium	Medium	High
Small incendiary	High	High	Medium	Low	Medium	High	Low	Medium	Low	High	High
Armed attack	High	High	High	Low	Medium	High	Low	High	Low	High	High
Unconventional weapon	High	High	Medium	Low	Low	Medium	Low	Low	Low	Medium	Medium
Sabotage	Medium	Low	Low	High	High	Low	High	High	High	Low	High
Hoax or threat	Medium	Medium	Medium	Low	Low	Medium	Low	Low	Low	Medium	High

RAND *MG705-A.2*

[3] Although such attacks are not impossible, a sufficiently large bomb placed above key infrastructure points could still damage them, if such attack points are available in a given rail system.

Consequences

Because information was not available on the disruption or damage that specific attack modes cause, the only quantitative measures that could be used to assess the likely consequences of individual attack scenarios were the injuries and fatalities caused in past attacks. We categorized the potential casualty consequences of attacks (1) using specific attack modes and (2) at specific locations in the rail system, based on the matrix shown in Figure A.3. Potential casualty consequences of attacks using a given weapon or at a given site were coded high if they produced *either* average numbers of injuries or fatalities above the average across all attacks (indicated in Figure A.3 by squares around the numbers) and were coded low or medium based on which half of the range between 0 and the average they fell. The categorization matrix was constructed this way to result in an attack mode or attack location being promoted to the higher of the two risk categories identified by its injury or fatality counts (e.g., having a high rating in *either* produced a high rating overall).

Using this categorization, both attack locations within the rail system (Figure A.1, schematic) were coded high, medium, or low based on the average injuries and fatalities that occurred as a result of attacks at that location (Figure 2.2 in Chapter Two), and attack modes were coded high, medium, or low based on the average number of casualties they produced (Table 2.3 in Chapter Two). Since these categorizations are based on past terrorist events, the ranking of attack modes and target locations that have fewer attacks in our data set is driven more strongly by the outcome of the few incidents that have occurred. Since our data set did not explicitly break out large from

Figure A.3
Consequence-Categorization Matrix for Attack Modes and Locations

Fatalities caused by attack:	Injuries caused by attack: 0–6	7–13	14–30
0–2	Low	Medium	High
3–4	Medium	Medium	High
5–8	High	High	High

RAND *MG705-A.3*

small bombs and incendiaries,[4] in this case, the large cases were moved up one consequence category from their small counterparts to reflect their potentially greater scale.

Two additional changes were made in rankings to address the limits in the available data. First, the consequences of unconventional weapons were set to high, given the wide uncertainty and potential high consequences from those attacks. Second, since our data set did not explicitly differentiate between casualties that occurred in attacks on different station types within systems (i.e., underground stations versus ground-level or elevated stations), the risk ranking of underground stations was increased one level to reflect the potential for attacks in such confined spaces to produce greater casualties. The results of these categorizations are included in Tables A.2 and A.3.

These two measures were combined to produce a casualty-consequence rating for using each attack scenario by applying the matrix in Figure A.4. This analytical step was designed to address the fact that the consequences of an attack scenario depend on both the weapon used and the site of the operation. Unlike the previous step, in which the goal was to choose the highest risk ranking based on either injuries or fatalities, here we wanted to produce a combined consequence score that reflected both the characteristics of the attack mode and location. As a result, the matrix was designed to average both results, though with a bias at the extremes—if an attack scenario had a high rating in either attack mode or site, it would have at least a medium consequence

Table A.2
Potential-Consequence Ranking of Attack Modes

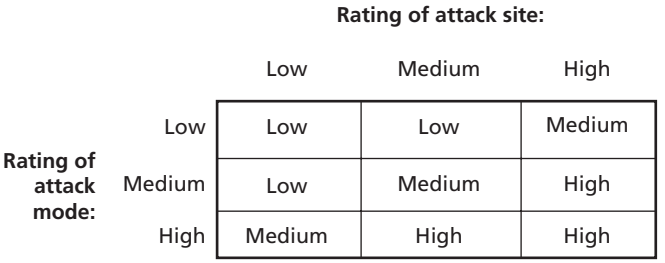
Attack Mode	Potential-Consequence Ranking
Large explosive	High
Small explosive	Medium
Large incendiary	Medium
Small incendiary	Low
Armed attack	High
Unconventional weapon	High
Sabotage	High
Hoax attacks or threats	Low

[4] Recent experiences with terrorist use of small-explosive devices in rail systems (e.g., London, Madrid, and Mumbai attacks) show the potential increase in damage that the use of multiple small devices simultaneously can produce. Since the unit of analysis for our risk ranking is single attacks, such complex incidents would be considered multiple single attacks being staged simultaneously. The potential for these weapons to be used this way can significantly increase the potential total consequences for their use.

Table A.3
Potential-Consequence Ranking of Attack Locations

Attack Location	Potential-Consequence Ranking
Weapon inside train	High
Underground stations	High
Station access or pathways	Medium
Underground infrastructure	Low
Trains underground (weapon outside train)	High
Ground-level stations	Medium
Ground-level track or infrastructure	Low
Ground-level or elevated trains (weapon outside train)	High
Elevated track or infrastructure	Low
Elevated stations	Medium
System-operation and power infrastructure	Low

Figure A.4
Casualty-Consequence Categorization Matrix



RAND *MG705-A.4*

rating, and, if it had a low in either, the highest it would be rated was medium. Figure A.5 presents the potential-casualty consequence rating for each attack scenario.[5]

Basing consequence assessments only on human casualties provides just part of the picture of the effects of terrorist operations. Although the desire to prevent casualties is frequently a major driver of security decisionmaking, the economic costs that attacks can produce are also a significant concern. As stated previously, no quantitative

[5] This result does not include whether it is *possible* to use each weapon at each site in the rail system. For example, even though it would be difficult to use a very large bomb inside a rail car, it is rated as high potential consequence, because, if it were done, it could produce very high casualties. These practical issues are addressed in the next step of the analysis, in which information on vulnerability and threat is combined with consequences to produce an overall risk score.

Figure A.5
Overall Potential-Consequence Ranking for Attack Scenarios, Based on Casualty Expectations

	Weapon in train	Underground stations	Station access and pathways	Underground infrastructure	Trains underground (weapon outside train)	Ground-level stations	Ground-level track or infrastructure	Ground-level or elevated trains (weapon outside train)	Elevated track or infrastructure	Elevated stations	System-operation and power infrastructure
Large explosive	High	High	High	Medium	High	High	Medium	High	Medium	High	Medium
Small explosive	High	High	Medium	Low	High	Medium	Low	High	Low	Medium	Low
Large incendiary	High	High	Medium	Low	High	Medium	Low	High	Low	Medium	Low
Small incendiary	Medium	Medium	Low	Low	Medium	Low	Low	Medium	Low	Low	Low
Armed attack	High	High	High	Medium	High	High	Medium	High	Medium	High	Medium
Unconventional weapon	High	High	High	Medium	High	High	Medium	High	Medium	High	Medium
Sabotage	High	High	High	Medium	High	High	Medium	High	Medium	High	Medium
Hoax or threat	Medium	Medium	Low	Low	Medium	Low	Low	Medium	Low	Low	Low

RAND *MG705-A.5*

data are available on economic consequences for the terrorist attacks in the sample data set. As a result, we lack a systematic basis for categorizing the potential economic consequences of each attack scenario in the same way we did for casualty counts.

In an effort to partially address this shortcoming of available data, the potential economic impacts of different attack scenarios were categorized based on a judgment of their likely economic costs, using such factors as the immediate reconstruction, repair, or replacement cost caused by the physical damage associated with the scenario and the disruption that the attack could cause in terms of the time it takes to restore system operations, with the first-order effect expressed in terms of the potential loss in operating revenues and the second-order effect being the longer-term impact in the eventual loss of daily operating revenues (and the broader economic benefits of the transit system), especially if people decide to take alternative forms of urban transit once rail-system operations are fully restored.

The general rationale for making consequence assignments included ranking larger attacks on more expensive targets more highly than smaller attacks on less expensive targets, actions that could cause destruction more highly than those that produced only disruption, actions that could affect the entire system more highly than those that could not, attacks that directly affected passengers more highly than those that did not, and attacks on elements of the system that could not be moved out of the way to restore functioning (e.g., stations as opposed to trains) more highly than those that could be relocated. While clearly imperfect, the fact that scenarios are being categorized only into high, medium, and low groupings helps reduce the impact of the obvious uncertainties in such a process. The results of this categorizing are shown in Figure A.6.

Figure A.6
Overall Potential-Consequence Ranking for Attack Scenarios, Based on Economic Expectations

	Weapon in train	Underground stations	Station access or pathways	Underground infrastructure	Trains underground (weapon outside train)	Ground-level stations	Ground-level track or infrastructure	Ground-level or elevated trains (weapon outside train)	Elevated track or infrastructure	Elevated stations	System-operation and power infrastructure
Large explosive	Medium	High	Medium	High	High	High	Medium	High	High	High	High
Small explosive	Medium	Medium	Medium	Medium	Medium	Medium	Low	Medium	Medium	Medium	Medium
Large incendiary	Medium	High	Medium	Medium	Medium	High	Medium	Medium	Medium	High	High
Small incendiary	Medium	Medium	Low	Low	Low	Low	Low	Low	Low	Low	Medium
Armed attack	Medium	Medium	Medium	Low	Low	Medium	Low	Low	Low	Medium	Medium
Unconventional weapon	High	High	Medium	Medium	Medium	High	Low	Medium	Low	Medium	Medium
Sabotage	Low	Low	Low	Low	Medium	Low	Low	Medium	Low	Low	High
Hoax or threat	Low	Low	Low	Low	Low	Low	Low	Low	Low	Low	Medium

RAND *MG705-A.6*

These two values for consequences were combined to produce a total net consequence estimate using the matrix shown in Figure A.7. Because of the significant uncertainty inherent in our estimates of the economic consequences of attack, the matrix was designed to make the consequence rating based on casualties dominant and to allow economic consequences to raise the overall estimate by only one class (i.e., for a scenario rated low for casualty consequences, an economic-consequence rating higher than low could raise the net consequence ranking only to medium; if the casualty-consequence ranking were medium, only a high ranking for economic consequences had any effect on the net rating, raising it to high).

The total net potential-consequence rating for each attack scenario is presented in Figure A.8.

Figure A.7
Total Net Consequence Categorization Matrix

		Rating of economic consequences:		
		Low	Medium	High
Rating of casualty consequences:	Low	Low	Medium	Medium
	Medium	Medium	Medium	High
	High	High	High	High

RAND *MG705-A.7*

Figure A.8
Overall Total Net Potential-Consequence Ranking for Attack Modes at Specific Rail-System Locations

	Weapon in train	Underground stations	Station access or pathways	Underground infrastructure	Trains underground (weapon outside train)	Ground-level stations	Ground-level track or infrastructure	Ground-level or elevated trains (weapon outside train)	Elevated track or infrastructure	Elevated stations	System-operation and power infrastructure
Large explosive	High	High	High	High	High	High	Medium	High	High	High	High
Small explosive	High	High	Medium	Medium	High	Medium	Low	High	Medium	Medium	Medium
Large incendiary	High	High	Medium	Medium	High	High	Medium	High	Medium	High	Medium
Small incendiary	Medium	Medium	Low	Low	Medium	Low	Low	Medium	Low	Low	Medium
Armed attack	High	High	High	Medium	High	High	Medium	High	Medium	High	Medium
Unconventional weapon	High	High	High	Medium	High	High	Medium	High	Medium	High	Medium
Sabotage	High	High	High	Medium	High	High	Medium	High	Medium	High	High
Hoax or threat	Medium	Medium	Low	Low	Medium	Low	Low	Medium	Low	Low	Medium

RAND *MG705-A.8*

Estimating Risk from Threat, Vulnerability, and Consequences

Estimating terrorism risk requires combining the estimates of threat, vulnerability, and consequences to provide an aggregate measure of the risk associated with specific attack scenarios. We do that by first combining threat and vulnerability scores into a single measure, and then combining that with the measure of potential total net attack consequences for each scenario.

Combining Threat and Vulnerability

A composite threat-vulnerability measure was produced by combining the threat score for each attack scenario (Figure A.1, based on historical terrorist use against specific rail targets) with the vulnerability score associated with each attack scenario described above. In an effort to focus our analysis on scenarios in which the most significant vulnerabilities exist in rail systems, when combining threat and vulnerability, we discarded all scenarios in which the vulnerability score was deemed low (Figure A.2). This was done through use of the matrix shown in Figure A.9, which explicitly eliminates such scenarios. This is consistent with our approach for scoring vulnerability, in which a rating of low was assigned to the least practical attack scenarios. In the matrix, there is a bias in categorization toward vulnerability (i.e., a medium-threat weapon in a high-vulnerability scenario is coded high, while a high-threat weapon in a medium-vulnerability scenario is coded only medium.) Figure A.10 shows the results of the composite scoring.

Figure A.9
Threat-Vulnerability Categorization Matrix

Threat ranking of attack mode:	Level of qualitative vulnerability: Low	Medium	High
Low		Low	Medium
Medium		Low	High
High		Medium	High

RAND *MG705-A.9*

Figure A.10
Composite Threat-Vulnerability Rankings for Attack Modes at Specific Locations in a Notional Rail System

	Weapon in train	Undergound stations	Station access or pathways	Underground infrastructure	Trains undergound (weapon outside train)	Ground-level stations	Ground-level track or infrastructure	Ground-level or elevated trains (weapon outside train)	Elevated track or infrastructure	Elevated stations	System-operation and power infrastructure
Large explosive			Medium			High	High	High	High	High	Medium
Small explosive	High	High	High	Medium	High	High	Medium	High	Medium	High	High
Large incendiary			Medium			Medium	Low	Medium	Low	Low	Medium
Small incendiary	High	High	Low		Low	High		Low		High	Medium
Armed attack	High	High	Medium		Low	High		High		High	Medium
Unconventional weapon	Medium	Medium	Low			Low				Low	Low
Sabotage	Low			High	High		High	High	High		Medium
Hoax or threat	Low	Low	Low			Low				Low	Medium

RAND *MG705-A.10*

Combining Threat, Vulnerability, and Consequences

An overall measure of risk combines threat and vulnerability with the potential consequences of particular attack scenarios. To do so, we combined the rankings included in Figure A.10 with the consequence estimates shown in Figure A.8, using the matrix shown in Figure A.11. In this case, the intent of designing the matrix was to combine the threat-vulnerability and consequence measures as closely as possible to equal, so it was structured similarly to the matrix for assessing casualty consequences in Figure A.4. The resulting aggregate risk estimates are shown in Figure A.12.

Figure A.11
Threat-Vulnerability-Consequence Categorization Matrix

Threat-vulnerability ranking:	Overall potential-consequence ranking: Low	Medium	High
Low	Low	Low	Medium
Medium	Low	Medium	High
High	Medium	High	High

RAND *MG705-A.11*

Figure A.12
Composite Qualitative Risk Rankings for Attack Modes at Specific Locations in a Notional Rail System

	Weapon in train	Undergound stations	Station access or pathways	Underground infrastructure	Trains underground (weapon outside train)	Ground-level stations	Ground-level track or infrastructure	Ground-level or elevated trains (weapon outside train)	Elevated track or infrastructure	Elevated stations	System-operation and power infrastructure
Large explosive			High			High	High	High	High	High	High
Small explosive	High	High	High	Medium	High	High	Low	High	Medium	High	High
Large incendiary			Medium			High	Low	High	Low	Medium	Medium
Small incendiary	High	High	Low		Low	Medium		Low		Medium	Medium
Armed attack	High	High	High		Medium	High		High		High	Medium
Unconventional weapon	High	High	Medium			Medium				Medium	Low
Sabotage	Medium			High	High		High	High	High		High
Hoaxes or threats	Low	Low	Low			Low				Low	Medium

RAND *MG705-A.12*

APPENDIX B

Cost-Effectiveness Assessment Details

Security-Improvement Option Cost-Estimating Details

Chapter Five provides a list of proposed SIOs divided into three categories (process-based improvements, technology-based alternatives, and infrastructure and facility modifications) along with investment and annual recurring costs estimated and average annual marginal costs calculated for each as Table 5.2 in that chapter. The same section in Chapter Five also discusses the details and the basis of the cost estimates for one illustrative SIO within each category. This appendix provides further details on the background of each of the proposed SIOs for the three categories, the data sources for the cost estimates, basis of estimates, and a description of the key cost drivers and other factors that contribute to the cost-range uncertainty of the estimates.

Process-Based Improvements

Implementing Enhanced Security Training (SIO 1.0)

Data Sources. The annual recurring costs per training session were based on cost data extracted from McCormick Taylor et al. (2006, Table 4).[1]

Basis of Estimates. This was previously discussed as one of three examples in Chapter Five.

[1] The FEMA training-cost information is based on data gathered from the Emergency Management Assistant Grant Program, State and Local Domestic Preparedness Exercise Support, and Emergency Management Performance Grants. The DHS G&T data are from the U.S. DHS Grant Program and Urban Area Security Initiative (UASI) Passenger Rail System Security Grant Program. Participants in the training programs listed are from transportation agencies, law-enforcement agencies, fire departments, emergency medical services, emergency management agencies or emergency operation centers, hazmat response units, media, public works and utilities, and vendors as actors (passenger victims), tenants in shared facilities, urban search and rescue, and volunteers. The costs from McCormick Taylor et al. (2006) were based on estimates provided by FEMA and the DHS G&T program office and other transportation agency staff interviewed by the authors. The FEMA and G&T costs to conduct training exercises were based on guidelines set by these two offices for typical consultant costs and simulation equipment. The authors also referred to those agencies' grantmaking offices, from which rail transportation agencies may be able to considerably offset their expenses for training programs.

Cost-Range Uncertainty. Even though we estimated the recurring cost based on the type of training and the frequency of classes and field exercises planned, the *actual* annual expenses of implementing enhanced security training can vary as needed.[2]

Adding a Canine Team (SIO 2.0)

Data Sources. Canine cost data were extracted from Balog et al. (2002).

Basis of Estimates. The investment cost is the one-time cost of procuring a team of six trained canines and kennels and other equipment and either modifying existing patrol cars or procuring three specially equipped K-9 patrol vehicles at between $10,500 and $55,500 each, with two canines and two K-9 patrol officers assigned to each vehicle.

The annual recurring cost is based on the estimated expenses of training and feeding the six canines over a two- to seven-year time frame assumed for maintaining a canine's level of effectiveness, paying and training the K-9 patrol officers as additional members of the existing rapid-response security force, and maintaining the equipment and servicing the three modified or new, specially equipped K-9 patrol vehicles over an assumed five-year service life before procuring a replacement.[3]

Cost-Range Uncertainty. In addition to including the initial training for certifying canine teams as part of the up-front investment cost, recurring training expenses were also included for recertification to be conducted as needed for the canines to develop the additional skills for detecting more unique types of explosive particles. The higher marginal-cost estimate of $700,000 includes the purchase cost and annual recurring expense of maintaining three specially configured patrol vehicles (with two canines and two K-9 officers per vehicle).

Instituting Background Checks and Issuing Upgraded Badges (SIO 3.0). For our notional baseline system, we also included the marginal cost of performing periodic background investigations for all rail-security, rail-operation, and maintenance personnel to identify whether any employees have previous criminal records. Even though this is not a standard practice across the case-study sites we visited, we added this option because one of the rail-operation managers we interviewed stated that the stake-

---

[2] For example, we discovered from our case-study site-visit interviews that there is an urgent need for training rail-security personnel at improving the postincident reporting process, so patrols can more quickly focus on the investigation and apprehension of terrorists. There was also an increasing need for rail-operation personnel to be trained in the latest reporting protocols and added responsibilities of being more highly visible and attentive across the station concourse and platform areas in creating a better partnership with the on-duty security officers. Also, we were told that one of the higher priorities in overall training of all rail personnel was the need for ensuring that they were aware of the most current set of emergency-preparedness and evacuation procedures, especially for ensuring that all the necessary resources can be quickly put in place to prepare for and contain a chemical or biological terrorist threat.

[3] Even though the marginal annual cost is based on dividing the investment costs for all the SIOs over the same five-year period, we also use the term *service life* here and for the other options to indicate when long-term investment plans and funds for procuring new replacement systems may be required, based on when system failures or degraded use are projected to occur.

holders have an obligation to carry out criminal-record investigations of their staff, including those employees working in the rail-network line-operation centers, IT personnel responsible for incoming train messages and rail-line status boards at the stations, and facility-maintenance personnel, among others. The intent of issuing new ID badges was for coding each one to provide a visual indication of the specific open and restricted areas of the system that each employee will have permission to access.

Data Sources. The cost of employee-background checks was extracted from LaTourrette et al. (2006). The investment costs of purchasing a badge-card printer and badges were based on quotes from Evolution Design Systems (undated) and Incode Corporation (undated).

Basis of Estimates. The investment cost is the one-time cost of procuring an ID-card printer at $2,500 and producing each badge at $1 each for the 2,000 rail-operation and security personnel.

The average annual recurring cost is based on the estimated expense of performing one initial background investigation per employee at an average of $150 each, with updates assumed every five years.

Increasing Signs at Stations and on Rail Vehicles and the Frequency of Public-Address Announcements (SIO 4.1). Increasing the number of signs within the concourse and platforms areas of all rail stations and on all the trains as well as adding more frequent public-address announcements (e.g., audible messages broadcasted throughout the station, trains, and open media) is intended to increase passengers' awareness to report any unattended baggage or any suspicious behavior to designated station operators or security officers.

Data Sources. Public awareness and LED display cost data were extracted from ITS (undated).

Basis of Estimates. There is a one-time total investment cost estimated at less than $10,000 for producing and installing signs in all the 47 stations and 360 rail vehicles in the inventory.

The total annual recurring cost is based on the expense of updating the signs over any given year and increasing the frequency of public-address announcements in the stations and rail vehicles and through the media (i.e., newspapers and radio), estimated at an average of $40,000 per year.

Installing Rail-Passenger Status LED Displays at All Stations (SIO 4.2). Our notional rail system does not currently have rail status–information LED displays installed in the stations. We included this option because, in addition to reminding passengers to report any unattended packages, the displays would also be capable of alerting passengers of any near–real-time updates of terrorist-warning awareness alerts, reported incidents across the system, and emergency evacuation information as needed. The LED displays also provide passengers with line status and train arrival information.

Data Sources. As with SIO 4.1, cost data were extracted from ITS (undated).

Basis of Estimates. The investment cost is the one-time cost of procuring and installing LED displays and communication fiber-optic lines and workstations for rail controller updates at between $4,000 and $8,000 each for each of the 47 stations.

The average recurring cost is based on the expense of maintaining the LED displays, fiber optics, and controller workstation, estimated to be approximately 10 percent of the total investment cost per year over a 10-year service life.

Cost-Range Uncertainty. The lower marginal annual estimate is limited to installing two LED displays at each of the 25 more heavily populated underground stations within the metropolitan area, and the higher estimate is based on applying the cost metrics to all 47 stations within our notional baseline system. The investment cost can also vary depending on the quality and size of the LED display and controller capabilities to make updates.

Technology-Based Alternatives

Installing Perimeter Fences and Adding Intrusion-Detection Systems (SIO 5.0). IDSs are used primarily for perimeter protection to monitor disturbances and set off alarms of potential terrorist attacks when a security breach occurs.[4] One case-study site we visited operates acoustic sensors as an IDS installed in all the rail tunnels. Infrared (IR) heat-seeking detection systems have also been installed to alert rail security of a breach in locating an unauthorized person trespassing within the tunnels or areas where trains have the right of way.

Data Sources. The cost of installing fences was extracted from Stevens, Schell, et al. (2004). The IDS cost data were extracted from Rowshawn and Simonetta (2003).

Basis of Estimates. This was discussed as one of three examples in Chapter Five.

Cost-Range Uncertainty. The IDSs procured are either (1) captive or fiber-optic cable, geophone, or tension fence-mounted sensors or (2) geophone, fiber-optic, or coaxial cable with buried, below-ground sensors. The lower marginal annual cost estimate is based on procuring, installing, and maintaining the less expensive, fence-mounted intrusion-detection sensors, and the higher estimate is based on using the more expensive, buried sensors.

Installing Passenger- and Baggage-Screening Systems (SIO 6.0). The stationary passenger- and baggage-screening systems are currently operating in a few multimode rail stations adjacent to airports. They have also been used in the past as part of a pilot program at selected stations at several rail sites.

Data Sources. Cost data for these screening systems were extracted from LaTourrette et al. (2006).

Basis of Estimates. The investment cost is the one-time cost of procuring and installing either (1) a minimum number of 26 stationary ion-mobility spectrometry-

[4] Even though we did not include this SIO for consideration in our notional rail system, IDSs can also be used on or adjacent to the fences assumed to be in place around the perimeter of the main power plant.

based (IMS) passenger- and baggage-screening systems at $150,000 each in 25 of the metropolitan underground stations, with an extra system going in the hub station to handle the additional volume of passengers during peak hours, or (2) a maximum number of 48 systems to screen passenger baggage at all 47 stations within the notional rail system. A TRL value of 9 was assessed for the stationary baggage-screening systems, as these systems have completed production and the costs are based on vendor quotes. The magnitude of the range estimate is based on the number of stations and the number of purchased systems per station, and the latter is based on a representative throughput rate of up to six passengers per minute per system.

The average recurring cost is based on the annual expense of (1) paying five security officers per system a full-time salary (40 hours per week for 52 weeks) for 24/7 baggage screening,[5] (2) training these officers, and (3) maintaining each system at $15,000 per year over the five- to 20-year service life.

Using Portable (Handheld) Detection Systems (SIO 7.0)

Data Sources. Surface acoustic wave (SAW) sensor cost data were extracted from Haupt, Rowshan, and Sauntry (2004). Electron-capture detector (ECD) cost data were extracted from Dun, Wood, and Martin (2005). We extracted IMS and SAW detector cost data from Derringer et al. (2006). Biological anthrax cost data were extracted from LaTourrette et al. (2006). For anthrax detectors, data were extracted from Ettehadieh (2006) and NIOSH (2003). Finally, optical chemical-seeker detector cost data were extracted from National Memorial Institute for the Prevention of Terrorism and RAND Corporation (ongoing).

Basis of Estimates. The investment cost is the one-time cost of procuring a minimum of 15 to a maximum of 30 portable (handheld) detection systems comprised of a sensor-mix purchase of the following:

- *explosive devices* (i.e., ECDs) at approximately $20,000 each to optical chemical-seeker detector at between $5,000 and $11,000 each that can also detect some chemical-warfare agents (CWAs)
- *chemical devices* with costs and performance varying from SAW sensors from $6,000 to $9,000 each that primarily detect CWAs to newer CWA-detector prototype devices projected in the $3,000 to $5,000 range that can also detect toxic industrial chemicals (TICs)
- *biological devices* (i.e., anthrax detectors) at $80,000 each, covering a limited area
- *IMS and SAW detectors* in the range of $25,000 to $35,000 each that detect primarily CWAs and TICs as well as some explosive particles.

[5] We assumed that the officers would have to be added for the notional rail system and not pulled from the existing rail-security and rapid-response team forces.

Current TRL values for portable (handheld) detection devices vary, with chemical and explosive devices assessed at values ranging from 4 (i.e., lab demonstrated) to 7 (i.e., on-site technology demonstrated) and biological devices assessed at a current value of 3 (i.e., undergoing proof of concept or feasibility testing). (Further details on specific devices and overall performance levels, including experienced detection and false-alarm and false-positive rates, are provided in the next section of this appendix.)

Since these detection devices would be fielded by the existing rapid-response teams of rail-security personnel, the average recurring cost is based on the average annual expense of (1) initial and follow-up training of personnel assigned from the rapid-response teams operating these devices at between $1,500 and $2,800 per officer and (2) maintaining each device, estimated to range from 25 percent of the investment cost to $5,000 to $6,000 annually for each portable (handheld) detector over a one- to three-year service life.

Cost-Range Uncertainty. To bound the estimate, the lower cost is based on procuring, operating, and maintaining a minimum mix of 15 portable (handheld) detection systems for performing random screenings with a unit procurement cost at the lower end of the range of estimated purchase prices. The higher estimate is based on procuring a maximum mix of 30 portable (handheld) detection systems for screening close to 100 percent of the passengers at one or more designated stations, with a unit procurement cost at the upper end of the range of estimated purchase prices.

Installing Perimeter Fencing and Adding Perimeter Surveillance Systems (SIO 8.0)

Data Sources. The cost of installing fences was extracted from Stevens, Schell, et al. (2004). Perimeter surveillance system cost data were extracted from ITS (undated).

Basis of Estimates. The investment cost is the one-time cost of procuring and installing (1) standard fencing with barbed or razor wire on top adjacent to the 30 miles of ground-level track at between $2 and $5 per linear foot and (2) a surveillance system mounted along the perimeter of fences every 1,000 ft, consisting of the following:

- color CCTV cameras at $3,000 each, along with improved illumination at $500 or a high-end thermal-imaging camera at $25,000 each
- video and image-control hardware at between $23,000 and $43,000 each
- power and data-transmission hardware at $1,200 to $4,400 each.

In addition, the investment cost includes the procurement and installation of (1) cable along the 30 miles of ground-level track and to the operation-control center at $1 per linear foot, (2) two video recorders at between $2,000 and $20,000 each, and (3) four workstation monitors at between $150 and $500 each. A TRL value of 9 was assessed for the perimeter surveillance system, as the CCTV cameras and other

hardware have completed production and the majority of the costs are based on vendor quotes.

The average recurring cost is based on the expenses of maintaining the fencing and cables estimated to be approximately 10 percent of the total investment cost per year over a 10-year service life, and the surveillance systems estimated at between 10 to 30 percent of the total investment cost per year over a three- to 10-year service life. We assumed that the rail-security personnel assigned to the operation-control center would be available to staff the colocated perimeter surveillance monitoring workstations.

Cost-Range Uncertainty. The lower marginal annual cost estimate is based on procuring, installing, and maintaining less expensive color CCTV cameras and additional lighting for the illumination needed. The higher cost is based on using more expensive, CCTV day and night thermal IR cameras. Both CCTV camera systems include the additional cost for remotely zooming in, tilting, and scanning.

Installing a Tunnel Surveillance System (SIO 8.1)

Data Sources. Similar to the costs of SIO 8.0, the cost of installing the tunnel surveillance system was extracted from Stevens, Schell, et al. (2004) and ITS (undated).

Basis of Estimates. The investment cost is the one-time cost of procuring and installing a surveillance system mounted inside the tunnel walls every 1,000 ft, consisting of the following:

- color CCTV cameras at $3,000 each, along with improved illumination at $500 or a high-end thermal-imaging camera at $25,000 each
- video and image-control hardware at between $23,000 and $43,000 each
- power and data-transmission hardware at $1,200 to $4,400 each.

In addition, the investment cost includes the procurement and installation of (1) cable along the 30 miles of tunnels and out through the underground stations and over to the operation-control center at $1 per linear foot, (2) two video recorders at between $2,000 and $20,000 each, and (3) four workstation monitors at between $150 and $500 each located at the operation-control center. The tunnel surveillance system was assessed at a TRL value of 9, as the CCTV cameras and other hardware have completed production and the majority of the costs are based on vendor quotes.

The average recurring cost is based on the expenses of maintaining the cables estimated to be approximately 10 percent of the total investment cost per year over a 10-year service life, and the surveillance systems estimated at between 10 to 30 percent of the total investment cost per year over a three- to 10-year service life. We assumed that the rail-security personnel assigned to the operation-control center would be available to staff the colocated tunnel surveillance monitoring workstations.

Cost-Range Uncertainty. The lower marginal annual cost estimate is based on procuring, installing, and maintaining less expensive color CCTV cameras and additional lighting for the illumination needed in the tunnels. The higher cost is based on

using more expensive, CCTV day and night thermal IR cameras. Both CCTV camera systems include the additional cost for remotely zooming in, tilting, and scanning.

Adding Rail-Vehicle Surveillance Systems (SIO 9.0). One of the case-study sites we visited has a plan in place to install CCTV cameras on each rail car as it is being pulled offline. Since rail cars have a service life of 20 to 30 years, new rail cars with the latest integrated, advanced technology seldom replace older rail cars. This is still the case even though one of the rail operators we interviewed stated that, in general, retrofitting trains is more expensive than integrating the latest security surveillance and other measures on new trains.

Data Sources. Rail-vehicle surveillance-system cost data were extracted from ITS (undated).

Basis of Estimates. The investment cost is the one-time cost of procuring and installing a surveillance system on each one of the 360 rail cars consisting of (1) two on-board CCTV cameras per vehicle at between $3,400 and $5,100 each and (2) a processor, GPS receiver for vehicle location, transponder, and wireless communication hardware at between $1,400 and $4,900 per vehicle. In addition, the investment cost includes the procurement and installation of two video recorders at between $2,000 and $20,000 each and four workstation monitors at between $150 and $500 each located at the operation-control center.

The average recurring cost is based on the expenses of maintaining the fencing and cables, estimated to be approximately 10 percent of the total investment cost per year over a 10-year service life, and the surveillance systems estimated at approximately 5 percent of the total investment cost per year over a five- to 10-year service life. We assumed that the rail-security personnel assigned to the operation-control center would be available to staff the colocated rail-vehicle surveillance monitoring workstations.

Upgrading Personnel Access-Control Systems (SIO 10.0)

Data Sources. Personnel ACS cost data were extracted from Rowshan and Simonetta (2003).

Basis of Estimates. The investment cost is the one-time cost of procuring and installing (1) either badge bar code or smart-card readers or magnetic-strip or optical scanners ranging from $500 to $5,000 each, (2) access-door control locks at $200 to $1,500 each, and (3) electrical connections using power and transmission hardware at $400 to $2,500 each and located at each of the restricted "rail and security personnel only" areas within each of the 47 stations as well as the operation-control center and power-plant facility. In addition, the investment cost includes the procurement and installation of cables installed at $1 per linear foot from each of these restricted areas to either a stand-alone, network-based, rail-personnel ACS at approximately $250,000 or a single, integrated system and database at approximately $4 million that is located and connected to cables within the operation-control center.

The average recurring cost is based on the expenses of maintaining the ACS estimated at between 5 and 10 percent of the total investment cost per year over a five- to seven-year service life and the rail-personnel ACS estimated at between 20 to 30 percent of the total investment cost per year over a five- to 10-year service life. We assumed that an adequate number of rail-security personnel assigned to the operation-control center would be available to staff the colocated rail-personnel ACS.

Cost-Range Uncertainty. The lower marginal annual cost estimate is based on using less expensive badge readers (e.g., bar-code scanners) and a lower end of the range estimated for a stand-alone, network-based, personnel ACS and database. The higher estimate is based on using more expensive personnel ACSs (e.g., retinal scanners) and a higher end of the range estimated for a single, fully integrated personnel ACS and database.

Implementing Hybrid Security Systems in Stations (SIO 11.0). The hybrid system that we estimated has two passive detectors installed at each station. If either of the two sensors detects a chemical particle, it automatically activates location-specific, enhanced CCTV cameras and sends a silent alarm along with real-time video data images from the station to the rail-operation control center. After a visual confirmation is made, the operation center can send out messages along with video data feeds to hazmat and other emergency-response teams. The teams can monitor the medical effects the attack is having on passengers and be better prepared with more effective methods to mitigate the situation once on the scene. Since there is also communication between the rail-operation control manager and the affected station operator and security officer, the hybrid system also provides early warning for rail personnel located within a restricted area at that location. The integrated chemical-detection surveillance imaging hybrid system also serves to provide a visual, archived record for supporting standard follow-up criminal investigations.

Data Sources: Cost data for the hybrid system were extracted from CUTR (2006).

Basis of Estimates. The investment cost is the one-time procurement and installation of a hybrid security system in each of the 25 metropolitan underground stations consisting of (1) passive chemical detectors per station (at between $15,000 and $25,000 each), (2) connected to enhanced surveillance CCTV cameras replacing outdated station cameras, and (3) fiber-optic links, all at an estimated total cost of between $160,000 and $1.4 million per station. The total cost varies depending on the square footage of each station, which drives the number of passive chemical detectors to procure. In addition, the investment cost includes networking the fiber-optic cables to four emergency management information system workstation monitors located within the operation-control center. Since the hybrid security system and costs are derived

from the currently fielded on-site demonstration of this system at selected D.C. Metrorail stations,[6] the TRL value for this system is assessed as a 7.

The average recurring cost is based on the expenses of maintaining (1) the chemical sensors (e.g., periodically replacing filters) and enhanced CCTV cameras at approximately $50,000 per station per year over a three-year service life and (2) the fiber optics and workstations at between 6 to 10 percent of the total investment cost per year over a five- to 10-year service life. We assumed that an adequate number of the rapid-response force security officers (e.g., hazmat team) and emergency responders would be available to assign to the operation-control center to staff the hybrid system's monitoring workstations.

Cost-Range Uncertainty. The lower marginal annual estimate is based on installing the hybrid system in the 25 stations within the metropolitan area, and the higher estimate is based on adding the system to the 22 rural stations within the notional baseline system.[7]

Facility or Infrastructure Modifications

Installing Blast-Resistant Containers (SIO 12.0)

Data Sources. Blast-container cost data were extracted from Blastgard International (2005).

Basis of Estimates. This was discussed as one of three examples in Chapter Five.

Installing Fixed Blast Barriers (SIO 13.1). Curbside-blast barrier installations can be phased in across stations depending on the passenger density at entrances around rush hours or the specific location of the stations relative to city-center areas of major business and commerce.[8]

Data Sources. Barrier cost data were extracted from LaTourrette et al. (2006), from quotes from Stonewear Force Protection for concrete or steel reinforced barriers. Alarm cost data were extracted from Rowshan and Simonetta (2003).

Basis of Estimates. The investment cost is the one-time procurement and installation of two 12-foot concrete-reinforced steel and sand blast barriers at between $100 and $200 per linear foot, sensor alarms at $5,000 to $20,000 each, and fiber-optic

---

[6] Security systems known as PROTECT were installed and operated as a pilot program at several WMATA Metrorail stations several years ago. Cost data were extracted from FTA (2006).

[7] The higher estimate also includes management reserve to account for the uncertainty of extracting costs reported for this pilot program operated at two rail stations, then scaling up the estimates to reflect the higher system quantity-buy cost savings and other economy-of-scale efficiencies.

[8] However, security officials we interviewed noted potential difficulties in installing blast barriers, since they may require retrofitting them for the existing curbside and sidewalk infrastructure to which they are adjacent. A potentially lower-cost security measure at street curbside entrances to underground stations within heavily populated metropolitan business districts is to restrict curbside parking or move taxi access to passengers to a greater standoff distance. Of course, unlike the blast barriers, this would not prevent a vehicle from being driven into a station.

cables at $3 per linear foot, all located at curbside entrances of all 25 metropolitan underground stations and 10 rural, ground-level stations.

The average recurring cost is based on training an available staff of rail-security personnel in monitoring the barrier-sensor alarm system, which we estimated annually at 5 percent of the total investment cost of the barrier systems over a 15- to 30-year service life.

Cost-Range Uncertainty. The lower and upper marginal annual estimates of installing barriers reflect quotes from different barrier-system suppliers that varied considerably based on the composition of the blast-resistant material they use and the type of alarm installed.

Installing Retractable Bollards (SIO 13.2)

Data Sources. Bollard cost data were extracted from Texas Security Gates (undated) that varied for permanent, ramp-style, fixed, vehicle barriers with chain reinforcements to hydraulic, retractable, metal bollards. Alarm cost data were extracted from Rowshan and Simonetta (2003).

Basis of Estimates. The investment cost is the one-time procurement and installation of one retractable bollard system at between $87,000 and $127,000 each at the curbside entrance to the building where the operation-control center is located and another at the entrance to the main power-plant facility.

The average recurring cost is based on training an available staff of rail-security personnel in monitoring the retractable-bollard alarm system, which we estimated annually at between 5 and 20 percent of the total investment cost of the bollard system over a 15- to 20-year service life.

Cost-Range Uncertainty. The lower and upper marginal annual estimates of installing retractable-bollard systems reflects differences in the two quotes from the system supplier for the two types of chain and hydraulic systems and different alarms available.

Installing Structurally Reinforced Pillars (SIO 14.0)

Data Sources. The cost data for installing pillars were extracted from Stevens, Schell, et al. (2004).

Basis of Estimates. The investment cost is based on procuring and installing structural concrete–reinforced pillars (or pilings) an equal distance between each existing pillar at between $7,700 and $15,700 each as part of the elevated infrastructure located at and supporting the 12 elevated stations and extending out another 0.25 mile on either side of each station to support the elevated rails.

We assumed that there was a sufficient number of rail-maintenance personnel available within the notional system to inspect and, as needed, repair the additional pillars, and that therefore there was no additional annual recurring cost required.

Cost-Range Uncertainty. The marginal annual range estimate reflects the lower- and upper-bound investment-cost estimates that can vary considerably, depending on site-specific construction contractors' quotes.

Effectiveness of Security-Improvement Options at Preventing Attacks Before They Occur

Chapter Five provides the assessment approach we took for assessing the effectiveness of each SIO at preventing attacks from occurring and specifically the ability to detect an attack before it takes place. This section provides a synopsis along with cited references of the performance of SIOs at detecting, quickly processing, and, if the results indicate, quickly responding to attacks before they occur. The assessment represents an independent, objective survey of various security practices and technology-based alternatives from information available from public sources. As we discuss below, any detection technique will have some measurable percentage of true positive detections and true negative detections, as well as false positives and false negatives.

Use of Canine Teams (SIO 2.0)

According to a rail-security respondent we interviewed at one of the case-study sites we visited, canine teams can currently detect 13 out of 21 different explosive ingredients on a potential terrorist's possession or clothing. The number of explosive ingredients detected in the future could increase. However, deploying canine teams (or patrols using portable (handheld) detection systems) to screen passengers at and around the station entrances will be more effective at reducing the probability of the incident occurring only if they can detect and quickly apprehend a terrorist before he or she detonates the explosives.[9]

Another drawback of the use of canines, especially in overcrowded parts of rail stations, is that the dogs may be easily distracted in this environment and would need to be rested often. On the positive side, the canine time to sample for a potential explosive device can take as little as 15 seconds. As far as detecting potential terrorists with firearms, canine teams have been known to be less reliable than portable (handheld) explosive-detection devices (SIO 7.0).

Use of Intrusion-Detection Systems Mounted on Perimeter Fencing (SIO 5.0)

With proper installation and calibration, IDS perimeter fence–mounted sensors can provide a low-nuisance alarm to warn rail operators and security personnel of breaches by unauthorized persons or potential terrorists.[10] IDS in-ground sensors can be installed adjacent to fences but may not perform comparably with the other sensors, especially when winter snow conditions are present, which may prevent detection of an intruder.

---

[9] According to one passenger-rail security officer we interviewed, there is an ongoing debate about whether to retrain these dogs to be more active rather than passive in sniffing out passengers. Even if this type of training is warranted and implemented, a question still remains: Even if a positive hit occurs, how does the canine team prevent the terrorist bomber from detonating himself or herself immediately in a crowded rail station?

[10] We assumed that, since an alarm is part of the overall system, a rapid-response team of security personnel would be available and required 24/7 to respond automatically as needed when the alarm is activated.

In addition, it is more difficult to service and replace in-ground sensors than it is to do the same for fence-mounted sensors.

The only other drawback reported is that some of the IDS sensors are highly susceptible to nuisance alarms or false positives from rain, snow, blown debris, animals, overgrown vegetation, and, for sensors mounted on perimeter fences, from rail maintenance touching the fences from the uncontrolled inside close to the railroad tracks. If these situations are frequent, it may be more desirable for these systems to be linked to video surveillance systems (SIO 8.0) to allow for visual confirmation of alarms.

Use of Portable (Handheld) Detection Devices (SIO 7.0)

Compared to stationary passenger- and baggage-screening systems (SIO 6.0), *portable (handheld) explosive-detection systems* have had very limited rail-system use and with minimal operational field data collected to date.

When compared to canine teams (SIO 2.0), the current open-source information available indicates that, in general, both SIOs provide the same medium number of false positives and false negatives and require between 15 seconds and one minute for sampling the passenger, backpack, or unattended baggage. Unfortunately, performance on both of these SIOs may not be the same, especially when attempting to detect large explosives inside vehicles, as vehicle surfaces may have been cleaned to remove explosive particles, which could foil detection. The only downside of canine teams compared to using portable (handheld) explosive-detection devices is that bomb-sniffing dogs may experience inconsistent levels of performance.

However, having stated this, it is still very difficult to accurately predict, with the same certainty, the operational performance of *portable (handheld) chemical, biological, or radiological detection systems* screening potential terrorists and detecting particles in their possession. Furthermore, the majority of the field-tested data that have been reported to date on both active and passive portable (handheld) detection systems indicated that most have the ability to operate effectively within relatively clean air environments or within a reasonable baseline set of acceptable conditions. Detection to prevent a chemical or biological attack from occurring is not possible using the currently available detectors, since there are throughput concerns of being able to effectively collect samples, analyze, and process the results in a timely manner.

One rail-security officer we interviewed at one of the case-study sites reported that the only way to test for biological hazards required removing and replacing the filters on a daily or more frequent basis; even after performing this maintenance, it was estimated to take between 16 and 24 hours or more to confirm a positive detection. Until the technology matures or can be adapted to work effectively within the worst-case underground station, the effectiveness of biological detectors is problematic.

However, if the overall objective is to detect and respond to airborne chemical and biological agents after they have been released, the detection devices can be useful at activating a silent alarm and launching countermeasures to shut off or open, as

appropriate, station air-ventilation systems, initiate evacuation procedures, and begin medical treatments to minimize the number of potential fatalities. The use of biological detectors would be very effective, as many agents produce no immediate symptoms and can be airborne for several hours before harming passengers, thereby allowing enough time for evacuation procedures to be implemented.

In general, the detection time required to mount an effective response depends on the agent and varies considerably for different agents. For a biological agent with a long incubation period, such as smallpox, a response time as long as a few days can still be beneficial. For a quick-acting chemical agent, such as sarin, a response time of a few seconds is needed.

Furthermore, as we discovered in our case-study review, there is still some uncertainty on how well detection systems will perform within underground and ground-level stations. Furthermore, transit-security personnel's level of training and ability to properly use, for example, a portable IMS will also be a factor in determining how well a positive detection of explosive or CWA can be done.[11]

As far as what devices have been field tested, several enhanced chemical-agent monitoring systems and software have been installed and used by rail security at a few stations as part of another pilot program. Field results indicated that the systems successfully detected possible classical nerve-gas and blister CWAs as well as blood and choking agents within a given underground station but did not address detection of the more commonly available TICs (e.g., chlorine and high concentrations of other cleaning agents).

Finally, one of the more promising devices is the IMS and SAW detection system, which can detect CWAs, TICs, and some explosive particles. This system has been field tested for detecting TICs and has experienced a rate of one out of five, or 20 percent, false positives in being able to detect latex paint, even when no indication of fumes was present. However, the IMS and SAW system has not been able to detect ammonia cleaner and has not been able to accurately detect air freshener 20 percent of the time when it was, in fact, present.

Use of Perimeter Surveillance Systems (SIO 8.0)

Thermal-imaging CCTV cameras have the advantage of providing both day and night surveillance capability but at more than nine times the investment cost of color CCTV cameras. If a more covert system is required, a thermal-imaging system, in which the camera requires no ambient light, may be a more preferable choice.

Video surveillance systems used for preventing perimeter incursions are now configured with software algorithms for providing a wide range of object-detection and tracking capabilities. This technology, known as *intelligent video surveillance*, is especially promising, since it has been exceedingly difficult and labor intensive for secu-

[11] Further information on IMS devices is provided in Stevens, Schell, et al. (2004).

rity staff to continuously monitor video imagery and detect anomalous events in real time.

Use of Blast Barriers and Retractable Bollards with Mounted Sensors and Alarms (SIOs 13.1 and 13.2)

Mounted sensors and alarms are included in the investment cost of installing fixed blast barriers and retractable bollards to minimize the presence or need for security personnel patrolling these areas. These sensors can detect damage and initiate alarms from the blast of nearby vehicle bombs and small explosives within relatively close proximity to the barriers and bollards. One type of sensor, geophone sensors, can also be installed and is capable of measuring the shock and vibrations on the barriers. However, the marginal costs of these sensors are higher, since they require the additional investment and maintenance cost of a dedicated processor to provide these measurements.

Lethality and Blast-Damage Assessments on Rail Passengers, Facilities, and Infrastructures

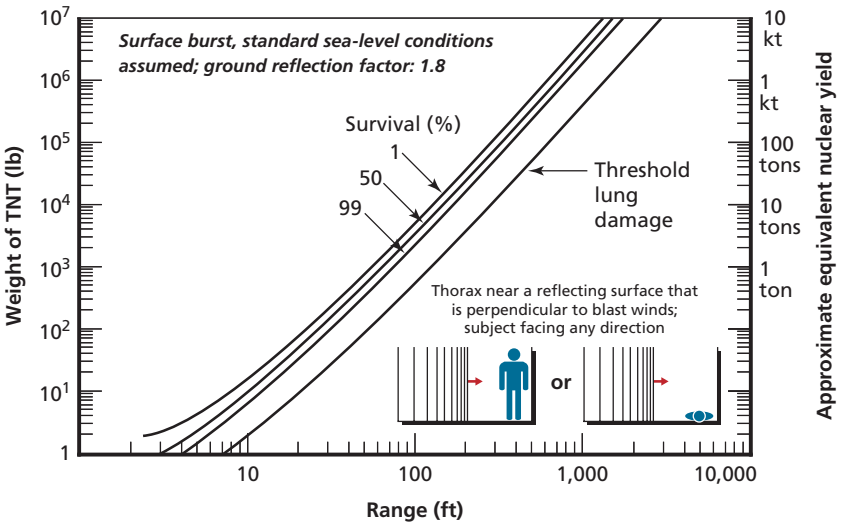
Chapter Five provides a discussion of step 2 of the cost-effectiveness assessment process for determining the relative improvement of each proposed SIO at averting fatalities and reducing the recovery times after a terrorist attack occurs over the baseline set of security measures for our notional rail system. Benchmark tables for these two damage-assessment metrics have to be generated before assessing relative improvements of each SIO. This section provides a summary of blast-damage assessment results for the impact on potential fatalities and injuries to rail passengers from small explosives to large vehicle bombs at various standoff distances from the location where the weapon is detonated, followed by a similar set of blast-damage assessment results to nearby rail, facilities, and infrastructures.

Potential Blast-Damage Effects on Passengers

The magnitude of potential fatalities is based on the likeliest size of the explosives (i.e., the TNT yields) from small-explosive, backpack-sized bombs to vehicle bombs, the effective blast-radius areas relative to where the detonation would take place, and the standoff distances and density of passengers within this radius. Based on previous RAND security research (Stevens, Schell, et al., 2004), Figure B.1 displays the survival rate and incipient lung damage of people for different levels of surface-burst TNT explosions.

A rather large bomb with a 5,000-lb TNT yield transported within a large van can create a surface blast for passengers within a ground-level lethal radius with a diameter between 88 and 110 feet, and can cause lung damage to passengers as far away as 170 to 210 feet. A smaller car bomb with a 500-lb TNT yield can result in

Figure B.1
Estimate of Tolerance to Direct Effects of Air Blast



SOURCE: Lovelace Foundation for Medical Education and Research and Defense Atomic Support Agency (1968).
NOTE: Predicted survival curves for a man exposed to surface blasts of TNT in which the thorax is near a flat, rigid surface that reflects the blast wave at normal incidence.
RAND *MG705-B.1*

a surface blast with a ground-level lethal radius for passengers within a diameter of between 38 and 56 feet and can cause lung damage to passengers as far away as 68 to 95 feet (Stevens, Schell, et al., 2004).

Figure B.2 illustrates the potential lethal radius and generic effects of potential injuries caused by a backpack-sized small explosive going off in a train station or train during typical rush-hour peak passenger densities.

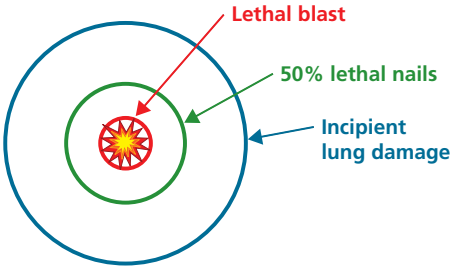
Calculations listed in the table in the lower part of Figure B.2 show that a 25-lb bomb produces lethal effects of potential injuries and fatalities from a blast of this magnitude at 13 feet, and, if the bomb is studded with nails, the resulting effects at 20 feet. Injuries are inflicted at more than 30 feet. The number of fatalities depends on the density of people. In a fairly overcrowded, highly dense, rail-platform area during rush hour, the number of fatalities could reach more than 100.

Potential Blast Damage to Rail Facilities and Infrastructures

Figure B.3 illustrates the blast damage to structures as a function of the size of the weapon yield (lbs of TNT) and the minimum standoff distance (in ft).

Figure B.3 displays the various standoff distances in a free field, where the incident overpressure (in psi) as a function of explosive weight displayed. Typically, a 100- to 1,000-lb bomb can be stored in an automobile, 1,000 to 4,000 lbs in a large

Figure B.2
Lethality of Small Explosives



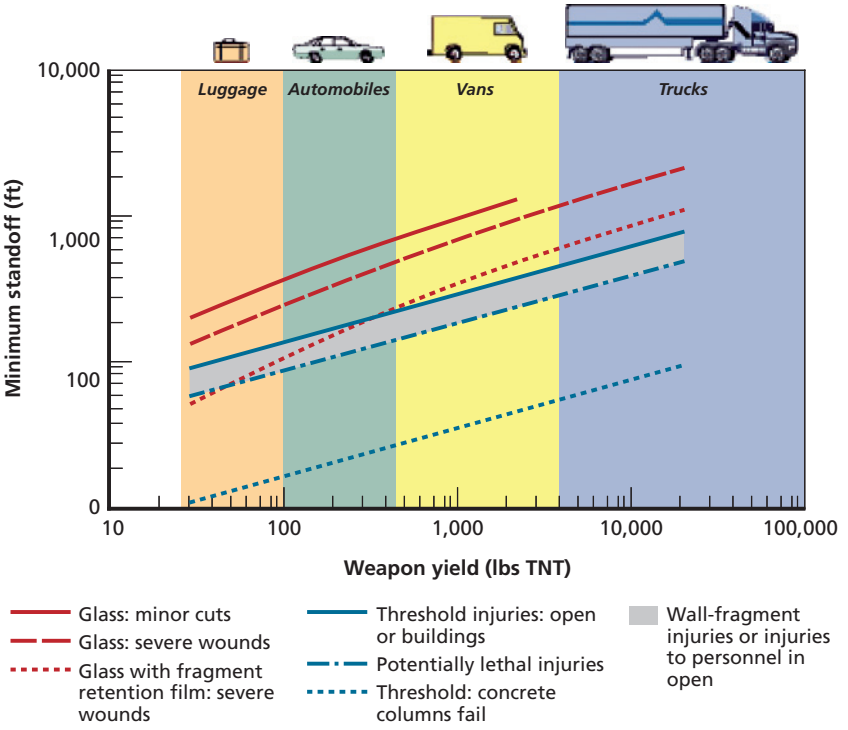
Explosive (lb)	Lethal blast (ft)	Injury blast (ft)	Lethal nails (ft^2)
5	3	11	250
10	7	18	500
25	13	30	1,250

	25-lb explosive effects		
Incidence (per ft^2)	Blast deaths	Blast injuries	Nail deaths
0.01	5	27	13
0.10	50	270	130

SOURCE: Stevens, Schell, et al. (2004).

RAND *MG705-B.2*

Figure B.3
Representative Blast Damage



SOURCE: FEMA (2003).

RAND *MG705-B.3*

van, and 5,000 to 10,000 lbs in a medium to large truck. The principal interpretation of this graph is that glass breakage occurs at overpressures of 0.15 to 0.22 psi and reinforced concrete walls or pillars supporting, for example, an elevated infrastructure without proper reinforcement can fail at 6 to 9 psi (Stevens, Schell, et al., 2004).

A van with a bomb with a 4,000-lb TNT yield and a car bomb with a 1,000-lb TNT yield can cause damage to the entrances and infrastructure of ground-level and underground rail stations, respectively, up to 640 and 400 feet away (Stevens, Schell, et al., 2004).

If an automobile containing a bomb is parked curbside adjacent to an infrastructure supporting an elevated rail station and within relatively close proximity to one or more supporting pillars, the blast would cause the roadway surface to crater. If a large van or truck containing a 5,000-lb TNT bomb exploded, it could cause a roadside crater up to 25 feet in diameter and with a depth of 4 ft (Stevens, Schell, et al., 2004).

A 1,000-lb TNT vehicle bomb would shear pillars within 15 feet, and a 2,000-lb TNT bomb would shear pillars as far away as 20 feet. The impact from the blast would cause the elevated rail-station structure to either be lifted off these sheared pillars, leading to severe cracking, or, in the worst-case scenario, completely collapse to the ground. The susceptibility and severity of this damage would be reduced if the existing pillars were extensively steel reinforced or additional steel-reinforced concrete pillars were added (SIO 14.0) to the infrastructure (Stevens, Schell, et al., 2004).

Implementing Security-Improvement Options Based on Cumulative Cost-Effectiveness Results

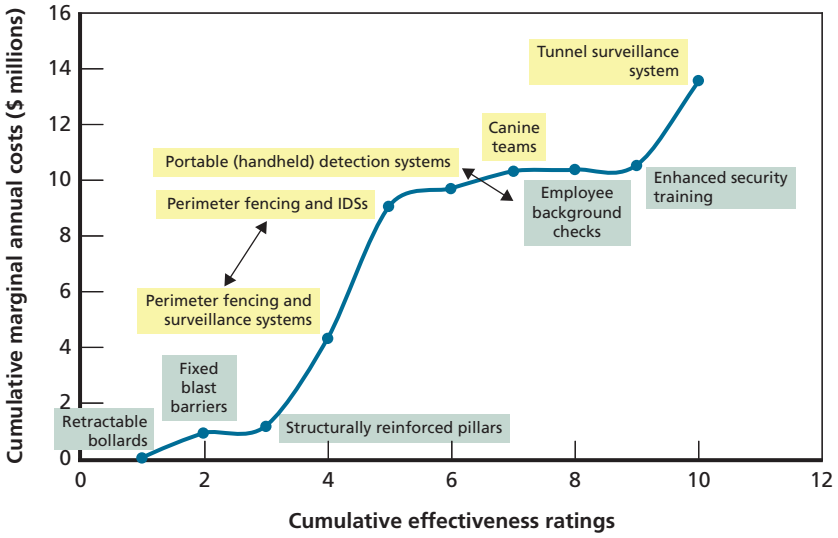
As mentioned in the section in Chapter Five that describes step 6 of the overall cost-effectiveness assessment process, we plotted the cumulative effectiveness-rating values (along the x axis) and the cumulative marginal annual cost (along the y axis) calculated from the information in Table 5.13 in that chapter to ensure that the order (from top to bottom) of implementing each preferred SIO listed on Table 5.14 in that chapter resulted in the maximum improvement in relative overall effectiveness at the lowest or moderate level of increased marginal annual cost.

Figure B.4 displays the plot of these data points for each of the SIOs capable of being effective against potential terrorist attacks at target locations across this security layer and with a total effectiveness-rating value greater than 0.0.

The options are listed in order from left to right in Figure B.4 with the highest overall effectiveness-rating value listed first. The steepness of the slope of the curve indicates the extent to which the relative improvement in effectiveness (or the higher the cumulative effectiveness-rating value) increases at a faster rate than the corresponding rate of

increase in cost (or the higher the cumulative marginal annual cost) for each option implemented.

Figure B.4
Cumulative Cost-Effectiveness of Perimeter-Layer Security-Improvement Options



NOTE: The colored labels next to each data point identify which SIOs ended up on the perimeter-layer preferred yes list (as green) and which SIOs were on the possible list for consideration at the system level based on the effectiveness rating per marginal cost values discussed as part of step 4 of the cost-effectiveness assessment process in Chapter Five.

RAND *MG705-B.4*

References

"7 July Bombings," *BBC News*, undated Web page. As of April 26, 2007:
http://news.bbc.co.uk/1/shared/spl/hi/uk/05/london_blasts/what_happened/html/default.stm

American Public Transportation Association, "Heavy Rail Transit Agencies Mileage and Stations Data," undated Web page (a). As of November 13, 2007:
http://www.apta.com/research/stats/rail/hrmiles.cfm

———, "Heavy Rail Transit Agencies Service and Usage Data," undated Web page (b). As of November 13, 2007:
http://www.apta.com/research/stats/rail/hrservuse.cfm

———, "Public Transportation Safety and Security Statistics," undated Web page (c). As of April 23, 2007:
http://www.apta.com/research/stats/safety/index.cfm

———, "Rail Definitions," undated Web page (d). As of April 23, 2007:
http://www.apta.com/research/stats/rail/definitions.cfm

———, "Rail Track Miles by Type," undated Web page (e). As of November 13, 2007:
http://www.apta.com/research/stats/rail/trackmilestype.cfm

———, *Public Transportation Fact Book*, 57th ed., Washington, D.C., 2006.

APTA—*see* American Public Transportation Association.

Associated Press, "Manhattan: Man Gets Five Years in Plot to Bomb Subway," *New York Times*, March 3, 2007. As of November 8, 2007:
http://www.nytimes.com/2007/03/03/nyregion/03mbrfs-bomb.html

Balog, John N., Peter N. Bromley, Jamie Beth Strongin, Annabelle Boyd, James Caton, and Don Corky Mitchell, *Public Transportation Security: A Guide for Decision Makers*, Vol. 2: *K9 Units in Public Transportation*, Washington, D.C.: National Academy Press, Transportation Cooperative Research Program report 86, 2002. As of November 14, 2007:
http://gulliver.trb.org/publications/tcrp/tcrp%5Frpt%5F86-v2.pdf

Berrick, Cathleen A., *Passenger Rail Security: Federal Strategy and Enhanced Coordination Needed to Prioritize and Guide Security Efforts: Testimony Before the Subcommittee on Homeland Security, Committee on Appropriations, House of Representatives*, Washington, D.C.: U.S. Government Accountability Office, GAO-07-459T, February 13, 2007. As of November 8, 2007:
http://purl.access.gpo.gov/GPO/LPS80711

BlastGard International, "BlastGard International Receives First Significant Order Valued at Around $735,000 from the Washington Metropolitan Area Transit Authority," press release, June 28, 2005. As of November 14, 2007:
http://www.blastgardintl.com/press/pr_062805.asp

Boardman, Joseph H., Administrator, Federal Railroad Administration, U.S. Department of Transportation, Testimony Before the U.S. House of Representatives Committee on Transportation and Infrastructure Subcommittee on Railroads, Washington, D.C., July 21, 2005. As of November 19, 2007:
http://www.fra.dot.gov/Downloads/PubAffairs/finaltestimony_07_21_05.pdf

Center for Urban Transportation Research, *Case Study: Washington Metropolitan Area Transit Authority (WMATA) District of Columbia*, Washington, D.C., FTA-FL-26-71054-03, undated. As of November 14, 2007:
http://www.cutr.usf.edu/security/documents/UCITSS/WMATA.pdf

Chalk, Peter, Bruce Hoffman, Robert T. Reville, and Anna-Britt Kasupski, *Trends in Terrorism: Threats to the United States and the Future of the Terrorism Risk Insurance Act*, Santa Monica, Calif.: RAND Corporation, MG-393-CTRMP, 2005. As of November 8, 2007:
http://www.rand.org/pubs/monographs/MG393/

Chow, James S., James Chiesa, Paul Dreyer, Mel Eisman, Theodore W. Karasik, Joel Kvitky, Sherrill Lingel, David Ochmanek, and Chad Shirley, *Protecting Commercial Aviation Against the Shoulder-Fired Missile Threat*, Santa Monica, Calif.: RAND Corporation, OP-106-RC, 2005. As of November 8, 2007:
http://www.rand.org/pubs/occasional_papers/OP106/

CUTR—*see* Center for Urban Transportation Research.

Derringer, Tricia, Thomas Kelly, Peter Bujnak, Robert Krile, Zachary Willenberg, and Eric Koglin, *S-CAD Chemical Agent Detection System*, U.S. Environmental Protection Agency Office of Research and Development, National Homeland Security Research Center, EPA 600/R-06/140, June 2006. As of November 14, 2007:
http://www.epa.gov/nhsrc/pubs/erSCAD112206.pdf

DHS—*see* U.S. Department of Homeland Security.

Dun, Sarah, Joseph Wood, and Blair Martin, *Decontamination, Cleanup, and Associated Issues for Site Contaminated with Chemical, Biological or Radiological Materials*, Washington, D.C.: U.S. Environmental Protection Agency Office of Research and Development, National Homeland Security Research Center, EPA/600/R-05/083, October 2005. As of November 14, 2007:
http://www.epa.gov/NHSRC/news/news102805.htm

Ettehadieh, Amir, Universal Detection Technology, telephone conversation with the authors, February 23, 2006.

Evolution Design Systems, "Evolution ID Card Systems and Badge Supplies," undated homepage. As of November 19, 2007:
http://www.evolution-1.com/

Federal Emergency Management Agency, *Primer for Design of Commercial Buildings to Mitigate Terrorist Attacks: Providing Protection to People and Buildings*, Washington, D.C., FEMA 427, December 2003. As of November 14, 2007:
http://www.fema.gov/plan/prevent/rms/rmsp427.shtm

Federal Transit Administration, "2006 Transit Watch Toolkit," undated Web page. As of November 8, 2007:
http://transit-safety.volpe.dot.gov/security/TransitWatch/toolkit2006.asp

Federal Transit Administration Office of Safety and Security, and John A. Volpe National Transportation Systems Center, *Transit Safety and Security Statistics and Analysis: 2002 Annual Report (Formerly SAMIS)*, Washington, D.C., December 2004.

FEMA—*see* Federal Emergency Management Agency.

FTA—*see* Federal Transit Administration.

Freeman, Alan, "Cities' Transit Systems Remain Easy Prey," *The Globe and Mail*, July 8, 2005, p. A9.

Friedman, Julia, *The District's Economy: Strengths, Weaknesses and Opportunity: The District Of Columbia Chamber of Commerce State of the Business Report*, Chris Knudson, ed., prepared for the 2007 Business Summit, June 2007. As of November 14, 2007:
http://www.dcchamber.org/clientuploads/2007_Biz_Report.pdf

Greenberg, Michael D., Peter Chalk, Henry H. Willis, Ivan Khilko, and David S. Ortiz, *Maritime Terrorism: Risk and Liability*, Santa Monica, Calif.: RAND Corporation, 2006. As of November 14, 2007:
http://www.rand.org/pubs/monographs/MG520/

Haupt, Steven G., Shahed Rowshan, and William C. Sauntry, *Public Transportation Security*, Vol. 6: *Applicability of Portable Explosive Detection Devices in Transit Environments*, Washington, D.C.: Transportation Research Board of the National Academies, Transportation Cooperative Research Program report 86, June 2004. As of November 14, 2007:
http://trb.org/publications/tcrp/tcrp%5Frpt%5F86v6.pdf

Hawley, Kip, Assistant Secretary, Transportation Security Administration, Department of Homeland Security, "Rail and Surface Transportation Security: Testimony Before the U.S. House of Representatives Committee on Homeland Security Subcommittee on Transportation Security and Infrastructure Protection," February 6, 2007. As of November 8, 2007:
http://homeland.house.gov/SiteDocuments/20070206172221-53276.pdf

Hoffman, Bruce, *Terrorism and Weapons of Mass Destruction: An Analysis of Trends and Motivations*, Santa Monica, Calif.: RAND Corporation, P-8039-1, 1999. As of November 8, 2007:
http://www.rand.org/pubs/papers/P8039-1/

———, "The Logic of Suicide Terrorism," *Atlantic Monthly*, June 2003. As of June 19, 2007:
http://www.theatlantic.com/doc/200306/hoffman

Incode Corporation, undated homepage. As of November 19, 2007:
http://www.incodenet.com/

ITS—*see* U.S. Department of Transportation, Intelligent Transportation Systems.

Jackson, Brian A., John C. Baker, Peter Chalk, Kim Cragin, John V. Parachini, and Horacio R. Trujillo, *Aptitude for Destruction*, Vol. 1: *Organizational Learning by Terrorist Groups and Its Implications for Combating Terrorism*, Santa Monica, Calif.: RAND Corporation, MG-331-NIJ, 2005. As of November 8, 2007:
http://www.rand.org/pubs/monographs/MG331/

Jackson, Brian A., Peter Chalk, Kim Cragin, Bruce Newsome, John V. Parachini, William Rosenau, Erin M. Simpson, Melanie Sisson, and Donald Temple, *Breaching the Fortress Wall: Understanding Terrorist Efforts to Overcome Defensive Technologies,* Santa Monica, Calif.: RAND Corporation, MG-481-DHS, 2007. As of November 8, 2007:
http://www.rand.org/pubs/monographs/MG481/

Jackson, Brian, A., Lloyd Dixon, and Victoria A. Greenfield, *Economically Targeted Terrorism: A Review of the Literature and a Framework for Considering Defensive Approaches*, Santa Monica, Calif.: RAND Corporation, TR-476-CTRMP, 2007. As of November 8, 2007:
http://www.rand.org/pubs/technical_reports/TR476/

Jenkins, Brian Michael, *Protecting Surface Transportation Systems and Patrons from Terrorist Activities: Case Studies of Best Security Practices and a Chronology of Attacks*, San Jose, Calif.: Norman Y. Mineta International Institute for Surface Transportation Policy Studies, San Jose State University, December 1997.

Jenkins, Brian Michael, and Larry N. Gersten, *Protecting Public Surface Transportation Against Terrorism and Serious Crime: Continuing Research on Best Security Practices*, San Jose, Calif.: Mineta Transportation Institute, San José State University, September 2001.

LaTourrette, Tom, David R. Howell, David E. Mosher, and John MacDonald, *Reducing Terrorism Risk at Shopping Centers: An Analysis of Potential Security Options*, Santa Monica, Calif.: RAND Corporation, TR-401, 2006. As of November 8, 2007:
http://www.rand.org/pubs/technical_reports/TR401/

"Leaders Condemn India Train Blast," *BBC News*, February 19, 2007. As of April 20, 2007:
http://news.bbc.co.uk/2/hi/south_asia/6375749.stm

Lengel, Allan, and Dan Eggen, "Metro Fire Was Plotted, Al Qaeda Member Says: Federal Officials Weighing Credibility," *Washington Post,* April 9, 2003, p. A8.

Libicki, Martin C., Peter Chalk, and Melanie Sisson, *Exploring Terrorist Targeting Preferences*, Santa Monica, Calif.: RAND Corporation, MG-483-DHS, 2007. As of November 8, 2007:
http://www.rand.org/pubs/monographs/MG483/

"London Attacks," *BBC News*, last updated August 15, 2007. As of April 27, 2007:
http://news.bbc.co.uk/1/hi/in_depth/uk/2005/london_explosions/default.stm

Lovelace Foundation for Medical Education and Research, and Defense Atomic Support Agency, *Estimate of Man's Tolerance to Direct Effects of Air Blast*, Washington, D.C.: Defense Atomic Support Agency, DASA 2113, October 1968.

"Madrid Train Attacks," *BBC News*, last updated February 14, 2007. As of April 27, 2007:
http://news.bbc.co.uk/2/hi/in_depth/europe/2004/madrid_train_attacks/default.stm

McCormick Taylor, Federal Transit Administration, Federal Highway Administration, National Research Council, Transportation Research Board, National Cooperative Highway Research Program, Transit Cooperative Research Program, Transit Development Corporation, and American Association of State Highway and Transportation Officials, *Transportation Security*, Vol. 9: *Guidelines for Transportation Emergency Training Exercises*, Washington, D.C.: Transportation Research Board, 2006. As of November 19, 2007:
http://trb.org/publications/nchrp/nchrp%5Frpt%5F525v9.pdf

Monterey Institute of International Studies, "ChemBio Weapons and WMD Terrorism News Archive," undated Web page (a). As of April 24, 2007:
http://www.nti.org/db/cbw/index.htm

———, James Martin Center for Nonproliferation Studies, "CNS Subjects: Chemical and Biological Weapons," undated Web page (b). As of November 19, 2007:
http://cns.miis.edu/research/cbw/index.htm

Murakami, Haruki, translated from Japanese by Alfred Birnbaum and Philip Gabriel, *Underground*, New York: Vintage, 2001.

National Institute for Occupational Safety and Health, *Guidance for Filtration and Air-Cleaning Systems to Protect Building Environments from Airborne Chemical, Biological, or Radiological Attacks*, Cincinnati, Ohio: Department of Health and Human Services, Centers for Disease Control and Protection, National Institute for Occupational Safety and Health 2003-136, 2003. As of November 19, 2007:
http://purl.access.gpo.gov/GPO/LPS66157

National Memorial Institute for the Prevention of Terrorism, and RAND Corporation, *RAND-MIPT Terrorism Incident Database*, Oklahoma City, Okla.: Oklahoma City National Memorial Institute for the Prevention of Terrorism, ongoing since 2002. As of November 8, 2007:
http://db.mipt.org/mipt%5Frand.cfm

Naval Civil Engineering Laboratory, *Terrorist Vehicle Bomb Survivability Manual*, Port Hueneme, Calif., 1988.

NIOSH—*see* National Institute for Occupational Safety and Health.

Orin, Deboray, John Mazor, and Andy Geller, "Feds Poi$on Apple: Subway-Cyanide Plot Proves It," *New York Post,* June 19, 2006, p. 4.

Rabkin, Matthew, Robert Brodesky, Frank Ford, Marsha Haines, Jordan Karp, Kristin Lovejoy, Terry Regan, Linda Sharpe, and Margaret Zirker, *Transit Security Design Considerations*, Washington, D.C.: Federal Transit Administration, 2004. As of November 8, 2007: http://transit-safety.volpe.dot.gov/Security/SecurityInitiatives/DesignConsiderations/CD/ftasesc.pdf

Rashbaum, William K., "Man Gets 30 Years in Subway Bomb Plot," *New York Times,* January 9, 2007, p. B1.

Riley, K. Jack, *Terrorism and Rail Security*, Santa Monica, Calif.: RAND Corporation, CT-224, 2004. As of November 8, 2007: http://www.rand.org/pubs/testimonies/CT224/

Rowshan, Shahed, and Richard J. Simonetta, *Public Transportation Security*, Vol. 4: *Intrusion Detection for Public Transportation Facilities Handbook*, Washington, D.C.: Transportation Research Board of the National Academies, Transportation Cooperative Research Program report 86, 2003. As of November 14, 2007: http://trb.org/publications/tcrp/tcrp%5Frpt%5F86v4.pdf

Sidell, Fred, "U.S. Medical Team Briefing," in U.S. Public Health Service Office of Emergency Preparedness, *Proceedings of the Seminar on Responding to the Consequences of Chemical and Biological Terrorism: July 11–14, 1995, Conducted at the Uniformed Services University of the Health Sciences, 4301 Jones Bridge Road, Bethesda, MD USA*, Bethesda, Md., 1996, pp. 2-30–2-35. As of November 8, 2007: http://purl.access.gpo.gov/GPO/LPS15853

Stevens, Donald, Thomas Hamilton, Marvin Schaffer, Diana Dunham-Scott, Jamison Jo Medby, Edward W. Chan, John Gibson, Mel Eisman, Richard Mesic, Charles T. Kelley, Jr., Julie Kim, Tom LaTourrette, and K. Jack Riley, *Implementing Security Improvement Options at Los Angeles International Airport*, Santa Monica, Calif.: RAND Corporation, DB-499-1-LAWA, 2006. As of November 8, 2007: http://www.rand.org/pubs/documented_briefings/DB499-1/

Stevens, Donald, Terry Schell, Thomas Hamilton, Richard Mesic, Michael Scott Brown, Edward W. Chan, Mel Eisman, Eric V. Larson, Marvin Schaffer, Bruce Newsome, John Gibson, and Elwyn Harris, *Near-Term Options for Improving Security at Los Angeles International Airport*, Santa Monica, Calif.: RAND Corporation, DB-468-1-LAWA, 2004. As of November 8, 2007: http://www.rand.org/pubs/documented_briefings/DB468-1/

Teamsters Rail Conference, *High Alert: Workers Warn of Security Gaps on Nation's Railroads*, Washington, D.C., 2005. As of November 19, 2007: http://www.teamster.org/divisions/rail/pdfs/railsecuritybook.pdf

Texas Security Gates, undated homepage. As of November 19, 2007: http://www.texassecuritygates.com

USACE—*see* U.S. Army Corps of Engineers.

U.S. Army Corps of Engineers Protective Design Center, "DoS and DoD Barrier Anti-Ram Vehicle Barrier Certification," last modified October 13, 2006. As of November 19, 2007: https://pdc.usace.army.mil/library/BarrierCertification

U.S. Department of Homeland Security, *Homeland Security Program Management Model for Technology Readiness Level (TRL) Assessment, Version 1.3,* Washington, D.C.: Science and Technology Directorate, September 1, 2005.

U.S. Department of Transportation, Intelligence Transportation Systems, "Unit Costs (Adjusted): Equipment Costs for Transit Management Center (TR)," undated Web page. As of November 14, 2007:
http://www.itscosts.its.dot.gov/its/benecost.nsf/SubsystemCostsAdjusted?ReadForm&Subsystem=Transit+Management+Center+(TR)

U.S. Environmental Protection Agency Emergency Response Program, "Sources of Common Contaminants and Their Health Effects," last updated September 17, 2007. As of November 19, 2007:
http://www.epa.gov/superfund/programs/er/hazsubs/sources.htm

Washington Metropolitan Area Transit Authority, *Washington Metropolitan Area Transit Authority (WMATA) Approved Fiscal Year 2007 Annual Budget Report*, October 2006.

Wedge, Dave, "Plot to Flood N.Y. Subway Tunnels Derailed, Secretary Urges Normal Use," *Boston Herald,* July 8, 2006, p. 4.

Wenck, Mary Anne, David Van Sickle, Dan Drociuk, Amy Belflower, Claire Youngblood, M. David Whisnant, Richard Taylor, Veleta Rudnick, and James J. Gibson, "Rapid Assessment of Exposure to Chlorine Released from a Train Derailment and Resulting Health Impact," *Public Health Reports*, Vol. 122, No. 6, November–December 2007, pp. 784–792.

Willis, Henry H., Andrew R. Morral, Terrence K. Kelly, and Jamison Jo Medby, *Estimating Terrorism Risk*, Santa Monica, Calif.: RAND Corporation, MG-388-RC, 2005. As of November 8, 2007:
http://www.rand.org/pubs/monographs/MG388/

WMATA—*see* Washington Metropolitan Area Transit Authority.