Homeland Security

This PDF document was made available from www.rand.org as a public service of the RAND Corporation.

Jump down to document ▼

The RAND Corporation is a nonprofit research organization providing objective analysis and effective solutions that address the challenges facing the public and private sectors around the world.

Support RAND

Purchase this document

Browse Books & Publications

Make a charitable contribution

For More Information

Visit RAND at www.rand.org

Explore the RAND Homeland Security Program

View document details

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

RAND

Homeland Security

The RAND Corporation is a nonprofit research organization providing objective analysis and effective solutions that address the challenges facing the public and private sectors around the world. RAND's publications do not necessarily reflect the opinions of its research clients and sponsors.

RAND® is a registered trademark.

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.