RESPONDING TO SECURITY THREATS IN THE POST-9/11 ERA
A Portrait of U.S. Urban Public Transit

BRIAN D. TAYLOR
CAMILLE N. Y. FINK
ROBIN LIGGETT
UCLA Institute of Transportation Studies

The 2001 terrorist attacks in the United States, and subsequent public transit system attacks in Madrid in 2004 and London in 2005, dramatically elevated concerns about the security of open, accessible transit systems. Accordingly, the authors report on a survey of 113 U.S. transit systems regarding their post-9/11 policies and practices. Sixteen of the 80 surveyed systems with rail service and/or enclosed bus or ferry terminals reported receiving a credible threat (e.g., bomb, chemical, biological, fire attacks) in the previous year, with most threats concentrated on just a few of the largest systems. Not surprisingly, attention to transit security increased significantly after 9/11, partly in response to federal mandates. Although attention to policing, security technologies, and public education all increased since 9/11, crime prevention through environmental design (CPTED) strategies increased the most. Despite measurable programmatic progress, however, many respondents believe that meaningfully securing urban transit systems remains a daunting, perhaps insurmountable, challenge.

Keywords: *terrorism; transit security planning; crime prevention through environmental design*

Brian D. Taylor is associate professor of Urban Planning and director of the Institute of Transportation Studies at UCLA, where he teaches courses in transportation policy and research design.

Camille N. Y. Fink is a PhD student in urban planning at UCLA, where she studies the social aspects of urban and transportation planning.

Robin Liggett is a professor of architecture, urban design, and urban planning at UCLA, where she teaches quantitative methods and software development.

Overview

When the September 11, 2001, attacks destroyed parts of the New York City transit system, the vulnerability of open, accessible U.S. public transit systems and their passengers to

AUTHORS' NOTE: This research was conducted with funding from the Mineta Transportation Institute at San Jose State University and the International Institute at UCLA; we are grateful for this generous support. Norman Wong of the UCLA Institute of Transportation Studies assisted with the design of the survey reported on here and developed and managed the Web-based survey system. Thanks also go to the other coauthors of the report from which this article is drawn (Anastasia Loukaitou-Sideris, UCLA; Martin Wachs, RAND Corporation; Ellen Cavanagh and Christopher Cherry, UC Berkeley; and Peter Haas, San Jose State University), the security and transit experts on our research project advisory committee members (Annabelle Boyd, Frances Edwards, Greg Hull, Brian Jenkins, John Sullivan, and Amy Zegart), and six anonymous referees for their helpful comments and suggestions on the report on which this article is based. Finally, we thank all the transit managers, chiefs of security, planners, and architects who took time to share their thoughts and opinions in our interviews and survey.

PUBLIC WORKS MANAGEMENT & POLICY, Vol. 11 No. 1, July 2006 3-17
DOI: 10.1177/1087724X06291133

terrorist acts was cast in the sharpest possible relief. Concerns about transit security have only heightened since the March 11, 2004, commuter rail bombings in Madrid, Spain, and the July 7, 2005, subway and bus bombings in London. Well prior to these dramatic attacks, however, research on terrorism and public transit had shown public transit systems worldwide to be the most common venue of all for terrorist acts.

Most previous research on transit terrorism has consisted of single or groups of case studies of major terrorist acts and responses to them by police and transit managers. Jenkins (1997) and Jenkins and Gersten (2001), for example, have conducted a series of case studies of terrorist attacks against international and domestic surface transportation systems, including networks in London, Paris, Tokyo, New York City, Atlanta, and the San Francisco Bay area. The analyses examine particular incidents, responses, and general security strategies, procedures, and training. These case studies are extremely useful, particularly in compiling "lessons learned" lists that can be applied to other transportation systems with similar physical and organizational characteristics.

Although often informative, case studies are limited in that they focus on individual events or systems and thus may not reflect the conditions or trends facing the transit industry more broadly. Thus, one cannot generalize from the findings of case studies, though in practice researchers often do (Yin, 2003). This is an especially relevant issue in the study of U.S. transit systems because they vary so dramatically in size—from thousands of vehicles and millions of daily passengers, to just a handful of vehicles carrying dozens of daily passengers. As potential targets of terrorist acts, these systems, and their stations and vehicles, are likewise dissimilar.

In contrast to case studies, aggregate analyses of data drawn from a representative sample of the population (in this case, larger U.S. transit operators) are generalizable and allow researchers to draw conclusions about the population under study (Singleton, Straits, Straits, & McAllister, 1988). However, more generalizable aggregate studies of the security experiences and practices of transit systems are rare. In the United States, just two such comprehensive aggregate studies of transit system security have been published in recent years.

In a 1997 Transit Cooperative Research Program report, Boyd and Sullivan (1997) described a survey of 42 transit managers regarding experiences with terrorist acts, perceptions of risks, and interagency coordination in planning for transit security. Boyd and Sullivan found that terrorist acts against transit systems were on the rise in the United States and worldwide, that transit agencies—particularly those operating rail service—were perceived by respondents to be at greater risk for attack than bus systems, and that coordinated efforts to both deter and respond to terrorist acts were on the rise but not commonplace.

Following the September 11, 2001, attacks, Congress asked the General Accounting Office (USGAO)[1] to consider what role the federal government should play in helping public transit operators reduce the likelihood and impacts of terrorist attacks on U.S. transit systems (U.S. General Accounting Office [USGAO], 2002). Part of this research included a mid-2002 survey of officials at 155 U.S. transit systems. The survey focused on security planning and preparation efforts, interagency and intergovernmental transit security coordination efforts, and perceptions of obstacles to more effective security planning. Perhaps it is not surprising to note, a principal finding of the 2002 USGAO report was that transit system managers surveyed cited increased funding as the most important role the federal government could play in assisting transit systems with security planning.

The findings of these two surveys, which are discussed in more detail in the pages that follow, contributed significantly to our understanding of the experiences with, perceptions about, and preparation for terrorist threats to U.S. transit systems. Although the 1997 Boyd and Sullivan survey was of a relatively small sample (60 systems surveyed, 42 responded) of transit systems, it provides a snapshot of transit systems when concerns about terrorist threats were just beginning to wax for many transit managers. The 2002 USGAO report surveyed many more transit systems (200 surveyed, 155 responded) about 6 months after the September 11th attacks, a time when transit managers (and, of course, their passengers) had a heightened awareness of terrorist threats, but before many new plans, programs, and procedures could be

put into place. Although both surveys devote considerable attention to bureaucratic, policing, and emergency response issues, they largely ignore the role of system design for transit security.

The survey reported on here complements and extends the findings of these two surveys in several ways. First, by surveying transit managers in the early summer of 2004, the survey findings provide a profile of experiences, perceptions, and actions nearly 3 years after the September 11, 2001, attacks made security a top priority among U.S. transit operators, and just after the largest single terrorist attack ever directed toward transit (in Madrid, Spain), which further heightened concerns about transit security. This allows us to examine the degree to which post-9/11 attention and federal initiatives and mandates have been integrated into transit planning practice.

Second, this research expands on these earlier studies by surveying respondents' attitudes toward and efforts in four distinct areas of transit security planning: (a) policing, (b) security hardware and/or technology, (c) public education and/or user outreach, and (d) environmental design strategies. The latter two of these approaches have received considerable attention in research on personal and property crime on transit systems, but far less in transit security research.

Finally, although previous research on transit system vulnerability has focused on transit systems operating one or more rail modes, less attention has been paid to systems that use or manage indoor bus, ferry, or other transit terminals. Like rail transit stations, terminals—such as the Port Authority Bus Terminal in Manhattan or the TransBay Bus Terminal in downtown San Francisco—host tens of thousands of weekday passengers in enclosed spaces vulnerable to terrorist attacks. We separately evaluate rail and nonrail transit systems below, however, we also include data on the experiences and perceptions of nonrail operators responsible for enclosed terminals.

Although previous research on transit system vulnerability has focused on transit systems operating one or more rail modes, less attention has been paid to systems that use or manage indoor bus, ferry, or other transit terminals.

Description of Survey

During the late spring of 2004, hardcopy and electronic letters describing our research and soliciting participation in a survey were sent to the general managers of all 259 U.S. transit agencies that, according to the National Transit Database maintained by the Federal Transit Administration (FTA), operate at least 50 vehicles in peak period service. The letter asked each general manager to designate the appropriate person or persons to complete an online survey. In the case of smaller systems, this was often the general manager himself or herself, and in larger systems this was most often (though not always) the director of policing or security. We assume in this analysis that the general manager was in the best position to determine who should complete the survey, so we do not parse our analysis to analyze responses by different types of respondents. The survey instrument was designed to allow each respondent the flexibility to complete the survey during the course of several interactive sessions before submitting a completed survey. Respondents from 113 transit agencies completed some or all of the survey questions (44% of the 259 agencies contacted). Details on the survey instrument and an analysis of the response rate and responding agencies are available at www.its.ucla.edu/security/reports/.

Given that many of the recent high-profile attacks on public transit systems in the developed world have been on trains or in enclosed rail stations, and the fact that many recent federal transit security initiatives have focused on the largest U.S. rail operators, we analyzed the survey results for (a) the entire sample, (b) rail and nonrail operators of large enclosed stations or terminals, (c) rail operators, and (d) nonrail operators without enclosed stations or terminals, and we report on these various categories below where appropriate or noteworthy.

Given this overview of the current sample, we now turn to the results of the survey, which is composed of three parts: (a) reported incidents and perceptions of threats, (b) efforts to assess threats and vulnerabilities, and (c) details on security planning efforts in four areas: policing, hardware and technology, public outreach and information, and environmental design strategies.

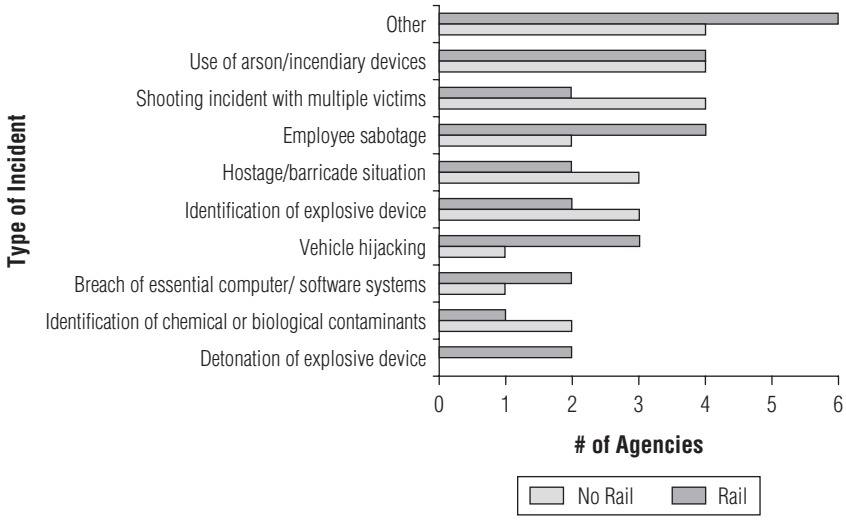

Figure 1: Types of Incidents Experienced by Systems

Incidents and Perceived Threats

Substantive security incidents on U.S. transit systems are rare, but not unprecedented.

Substantive security incidents on U.S. transit systems are rare, but not unprecedented. Respondents were asked about the occurrence of various types of security incidents, and the frequency of such incidents during the past decade. The results of this query track very closely with those reported in 2002 by the U.S. Government Accounting Office (USGAO; 2002) suggesting some reliability in the results. Agencies with rail systems (n = 28 or 25% of respondents) or nonrail systems with enclosed terminals (n = 52 or 46% of respondents) were asked about possible terrorist incidents experienced on their systems. Of these 80 systems queried, there were 68 valid responses. A total of 28 agencies reported experiencing some sort of incident, 12 of these were rail transit systems, and 16 were nonrail operators. Counts of different types of incidents experienced are shown in Figure 1. Use of arson and/or incendiary devices on a system was the most common type of incident recorded. The Other category included reports by two systems of suspicious packages that, when identified, turned out to be false alarms, a bomb threat, two knife attacks, a shooting with no victims, theft of a radio system, hazardous materials contamination on a bus, and a case of rail track tampering. Details on these incidents are summarized in Table 1.

Respondents at 16 agencies indicated that they had received one or more of what they believed to be credible threats (e.g., bomb, chemical, biological, fire attacks) in the past year. Most of these (14 of the 16) had received from one to four threats. Two other very large rail operators reported large numbers of threats; one cited 31 credible threats in the past year, and the other 12.

In addition to providing information on actual threats and attacks, respondents were also asked about their perceptions of vulnerabilities. Although one could argue that these survey respondents (who were designated by each system's general manager as the person at that agency who is most knowledgeable about transit security issues) are in perhaps the best position of anyone to offer vulnerability assessments, such perceptions should probably be treated more as informed speculation than concrete assessments of vulnerability. What is most clear from responses to these questions, however, is that transit systems are, by their very nature, perceived by system managers as very vulnerable to terrorist attacks. Of respondents who expressed opinions on vulnerability, only in the case of paratransit did fewer than 60% of the respondents rank a transit mode or system component as somewhat or very vulnerable. Overall, rail modes were perceived by respondents to be the most vulnerable, though these

Table 1: Description of Incidents

Type of Incident	*System Has Rail*	*# of Incidents in Last Decade*	*Year of Most Recent Incident*	*Location of Incident*	*Description of Incident*
Identification of explosive device on system	No	1	2002	Bus stop	Pipe bomb placed in trash can was located and destroyed.
	Yes	1	2002	Vehicle	Suspicious package on bus removed from vehicle.
	Yes	< 12	—	Station	Pipe bomb found on rail transit platform.
Detonation of explosive device on system	No	1	2003	Vehicle	Explosive device detonated by juveniles on a bus.
	No	1	2004	Station	Soda bottle bomb was detonated on a bus at main transfer point injuring one passenger.
Use of arson and/or incendiary devices on system	No	3-4	2003	Vehicle	Juveniles playing with matches ignited various things.
	No	Several	Yearly	Vehicle/bus stop	Arson vandalism by juveniles.
	No	—	2003	Bus stop shelter	Juvenile lit a bus stop shelter on fire.
	No	1-2	—	Station	Fire started in restroom trash container.
	Yes	120	2004	Station/vehicle	Intentional lighting of newspapers to make a fire.
	Yes	3	2002	Bus/train	Five buses destroyed by fire and 3 more damaged.
	—	—	—	—	Rail car seat set on fire.
	Yes	1	2002	Vehicle	Fire intentionally started on floor of vehicle.
Chemical or biological contaminant	No	1	2003	Vehicle	Suspect sprayed pepper or mace on board.
	Yes	20	2002-03	Vehicle	White powder anthrax scare.
Vehicle hijacking	No	—	2002	Vehicle	Intoxicated male assaulted driver and attempted to leave using vehicle.
	No	1	1988	Vehicle	Passenger wanted to go to a city where the bus did not go. No other passengers were on board.
	No	1	1994	Vehicle	Passenger who said he had a gun demanded to be taken to the airport. He was arrested there.
	Yes	1	2004	Vehicle	Passenger took control of bus when it started back to the location where he boarded.
Hostage and/or barricade situation	No	1	2003	Vehicle	Armed suspect boarded a bus. Shots were exchanged with no injuries and suspect captured.
	No	1-2	2004	Vehicle	Passenger told driver he had a bomb strapped to his chest. Police were notified by silent alarm. There was no bomb.

(continued)

Table 1 (continued)

Type of Incident	*System Has Rail*	*# of Incidents in Last Decade*	*Year of Most Recent Incident*	*Location of Incident*	*Description of Incident*
	Yes	—	—	Station	Incident at rail station handled by local law enforcement.
	Yes	2	1999	Vehicle	Mentally disturbed persons threatening to harm others.
	Yes	1	—	Bus terminal	Man barricaded in coffee shop threatening to kill himself. Surrendered after negotiations with police.
Employee sabotage	No	Several	2004	Vehicle/bus garage	Miscellaneous instances.
	No	—	2003	Maintenance facility	Sabotaged oil on several revenue and support vehicles.
	No	—	2003	Vehicle/bus garage	Removal of microphones; damage to cameras.
	No	—	—	Station	Disabled buses.
	Yes	1	1985	Building	Employee drove stolen vehicle into administration building.
Breach of computer and/or software systems	No	Several dozen	2004	Vehicle	Sabotaging digital cameras and/or audio devices.
	No	—	2004	Other	Computer viruses.
	Yes	1	2003	Computer	Accidental hacking caused brief shutdown of operations.
Shooting incident with multiple victims	No	1	2002	Vehicle	Male passenger boarded bus with shotgun and shot another passenger and himself.
	No	1	—	Other	North Hollywood shootout.
	Yes	1	1996	Station	Gang members shot other gang members in stairwell at entrance to the station.
	Yes	1	1994	Station	Person shot two or three passengers at station.
	Yes	—	—	Maintenance facility	Disgruntled employee went to work and started shooting.
Other	No	2-3	2002	Vehicle	Passenger told bus driver he had left a bomb on rear seat and ran away.
	No	2	2004	Outside vehicle	Vehicle windows shot out while traveling on road.
	No	3	2004	Multimodal transfer center	Suspicious bag left on bench. Terminal evacuated until bomb squad determined it was not a bomb.
	No	2	2000	Vehicle	Chemicals for methamphetamine production released accidentally.
	No	1	2004	Vehicle	Radio stolen from service vehicle and vehicle set on fire.
	No	1	2004	Vehicle	One passenger stabbed another after verbal altercation.
	Yes	1	2003	Tracks	Track jacked up and boulder placed under track.
	Yes	—	2004	Vehicle	Operator shot by estranged husband.
	Yes	2	2001	Station	Two planes hit the World Trade Center Towers causing a collapse onto station.
	Yes	< 10	2004	Vehicle	Male climbed through bus window and robbed driver.

findings are based on relatively few responses. Finally, respondents collectively did not assign much difference in vulnerability ratings of various system components.

Given this overview of actual and perceived security threats in the current sample of U.S. transit systems, we now turn to the security planning efforts of these systems.

THREAT AND VULNERABILITY ASSESSMENTS

Of the 113 agencies represented in the sample, 85% indicated that they had conducted some level of threat and vulnerability assessment of key system infrastructure. This is a significant increase over the 54% reported by respondents to the 2002 U.S. General Accounting Office survey, likely reflecting the fruits of federal policy mandates for such assessments. Agencies with rail were much more likely than nonrail operators to have conducted a comprehensive assessment; almost half (46%) of the agencies with rail in the current sample reported that they had conducted a comprehensive security assessment as of the summer of 2004, compared to only about 13% of agencies without rail.

Transit agencies without rail in the current sample that had conducted some sort of a security assessment most often described theirs as moderate or partial assessments, rather than comprehensive. Among nonrail systems, we find little difference in the assessment practices between those with multimodal transfer facilities or enclosed bus terminals, and those without—suggesting that nonrail systems operating large, enclosed, and perhaps vulnerable facilities may be slipping through the cracks with respect to threat and vulnerability assessments.

Among those systems that have not conducted security assessments, the primary reasons given for not doing so were lack of resources or the fact that services were contracted to an outside agency. Four agencies indicated that they were in the process of planning an assessment at the time of the survey, while one respondent stated simply that his or her agency was not a "high value target."

HOW OFTEN?

Thirty-five agencies reported conducting assessments at least once a year, whereas 28 agencies report conducting assessments every 2 or 3 years. The remaining agencies report no regular policy regarding frequency but rather conduct assessments as deemed necessary. Of agencies conducting assessments, 70% had done so in the past 2 years. In general, the reported frequency of such assessments is substantially higher than was reported in the USGAO survey just 2 years earlier—again likely reflecting aggressive post-9/11 initiatives and mandates. There was no significant difference in the timing of assessments between agencies that operate rail and those that do not.

PURPOSE AND USE OF ASSESSMENTS

The most common purposes reported for the most recent threat and vulnerability assessment conducted were to assess terrorism-related vulnerabilities (80%) and crime-related vulnerabilities (70%). Only 38% of the systems reported using such efforts to assess natural disaster–related vulnerabilities, which contrasts significantly from the 85% reported in the 2002 USGAO survey. (Given the recent attention to the vulnerability of transit systems to natural disasters such as Hurricane Katrina, we expect to see the policy pendulum swing back toward increased assessments of natural disaster vulnerabilities in the next few years.) Other assessment purposes reported were to assist in developing a security plan and to help prioritize security enhancements for implementation. All but one of the systems with rail (96%) mentioned terrorism as a purpose of the assessment as compared to three fourths of systems without rail. Furthermore, among systems without rail there were essentially no differences in the stated purposes of the assessments between systems that operated a multimodal transfer or enclosed bus terminal and those that did not.

Identifying effective security and technology procedures and supporting decision making at the executive level were the most prevalent uses of the threat and vulnerability assessment results reported. Almost all systems with rail have multiple uses for the assessment results and are much more likely to use the assessment for the specific uses listed in the survey than are systems without rail. For example, 62% of systems with rail use the assessment results in applications for Urban Area Security Initiative grants, as compared to only 6% of systems without rail or an enclosed transfer facility.

WHO CONDUCTS ASSESSMENTS?

About one third of the agencies without rail reported solely using an in-house team to conduct their threat and vulnerability assessments, while only 12% of systems with rail conducted such assessments in-house, likely reflecting the FTA's Security Technical Assistance program targeted at the 50 largest U.S. transit systems. Systems with rail were more likely to use a combination of groups to conduct the assessment, primarily made up of an in-house team along with contracted security consultants. Systems without rail were twice as likely to use the sheriff's or police department (about one third) than systems with rail (16%). The most common Other group mentioned was assistance from the FTA (listed by 9 agencies).

ONGOING ASSESSMENT

Respondents were asked to describe other ways their agency attempted to identify and assess security vulnerabilities in the transit system. Most frequently mentioned were constant monitoring of crime statistics, periodic reviews and/or discussions of security by employees, daily visual checks and/or observations, employee and customer feedback, and regular contact with local law enforcement agencies. Many agencies reported having an internal security committee that meets on a regular basis to discuss and monitor security.

Given this review of types, frequencies, and goals of security planning efforts, we now turn to the use and extent of four types of security strategies.

OVERVIEW OF SECURITY STRATEGIES EMPLOYED

Respondents were asked about their views on the importance of each of four, distinct categories of security strategies, and whether these views had changed since September 11, 2001:

- Policing
- Security hardware and/or technology
- Public education and/or user outreach
- Environmental design strategies

The percentage of respondents who believe that all four of these strategies are central to security planning nearly doubled after 9/11 (see Figure 2). Before and after 9/11, however, policing was considered the most central strategy, followed by security hardware and/or technology. Neither public education and/or user outreach nor environmental design strategies were given much importance by respondents before 9/11. Following 9/11, however, respondents from more than one half of the agencies said that these factors had become significant and even central parts of security planning. Although attention to security increased for all types of transit agencies following 9/11, all four of the strategies analyzed here (policing, technology, public education, and design) were considered more significant or central to security planning for agencies with rail than for agencies without.

Before 9/11, respondents from agencies with rail were much more likely to have considered policing significant or central to security planning than those from agencies without rail (see Figure 3). Following 9/11, however, most respondents from both types of agencies thought

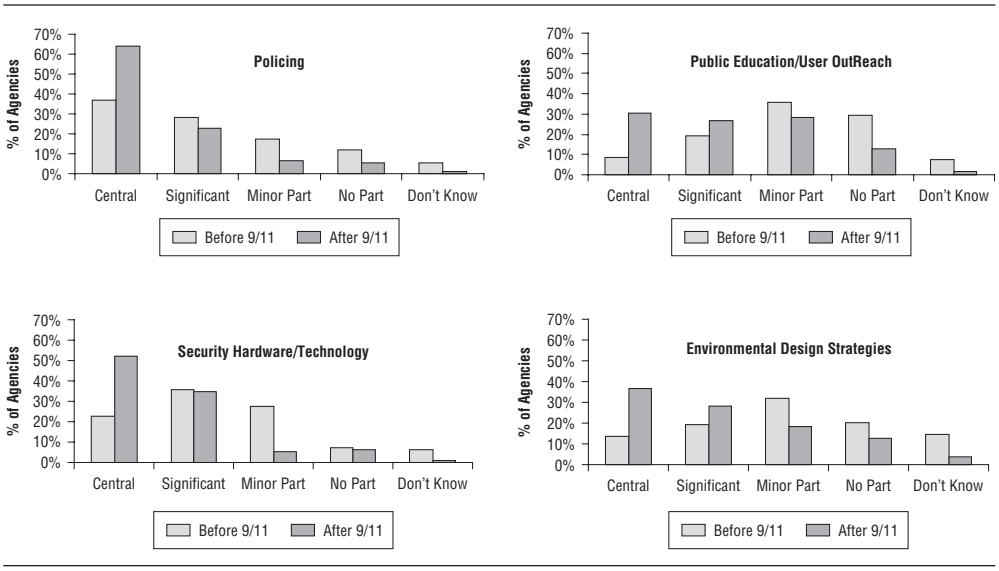

Figure 2: Importance of Strategies in Security Planning

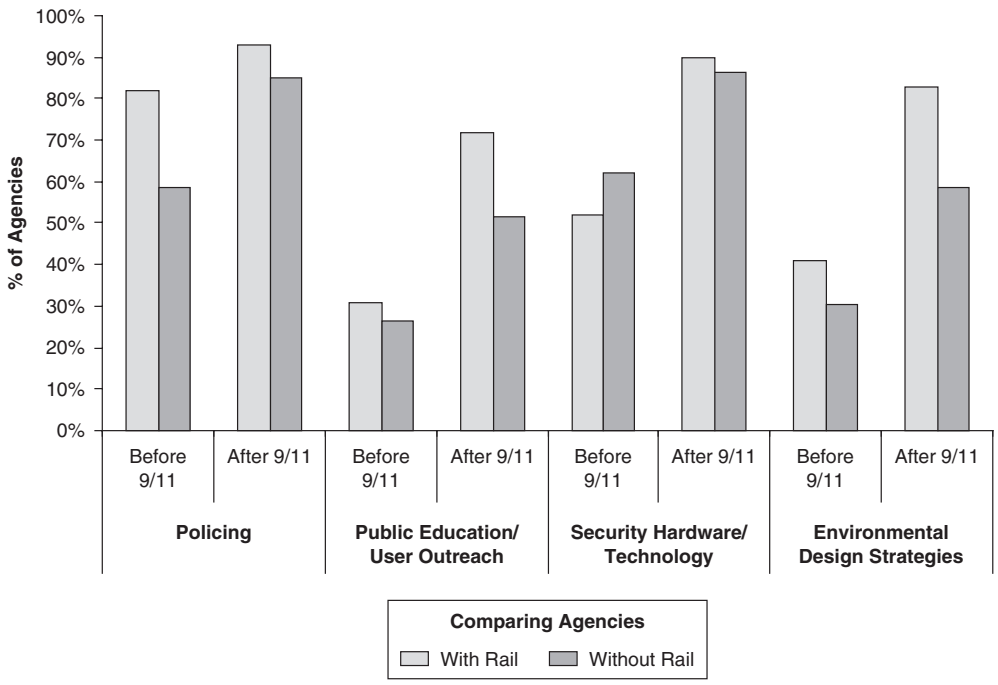

Figure 3: Strategies Considered Central or Significant in Security Planning

policing to be a significant or central strategy. Environmental design strategies were considered by respondents from agencies with rail to be a more significant part of security planning, before and after 9/11. Given that operators of rail systems are likely to be responsible for securing many rail stations and miles of rail rights-of-way, this result is not surprising. By contrast, nonrail operators of enclosed stations or terminals typically operate just one or few such stations and are not responsible for securing the streets and sea lanes on which their vehicles operate.

When asked about specific changes in security strategies after 9/11, many respondents reported that increased resources (i.e., funding) were now devoted to policing strategies. For some agencies this entailed the development of a new in-house police or security force; in other cases, where police forces were already in place, the number of police and/or security officers increased. Specifically, many respondents reported having a greater public police presence with greater attention paid to increased public visibility of police officers and security guards. In addition, many respondents reported increased coordination with local law enforcement, and increased employee awareness training regarding the vulnerabilities of systems to terrorism.

Following 9/11, agencies have tended to look for new ways to engage passengers on security issues. A number of agencies have implemented a Transit Watch program, promoted by the FTA, to engage the public as additional security "eyes" and "ears." Others have sought to increase public awareness of security issues through posters, pamphlets, Web pages, and regular newsletters.

The most common change in security hardware and/or technology strategies reported after 9/11 is the increased use of surveillance cameras on vehicles and at stations. Also more electronically controlled access points have been implemented.

Respondents reported greater awareness of and attention to crime prevention through environmental design (CPTED) strategies after 9/11.

Finally, respondents reported greater awareness of and attention to crime prevention through environmental design (CPTED) strategies after 9/11. Although awareness of CPTED strategies was high, few agencies reported actually implementing CPTED strategies post-9/11. Such a result is not surprising, however, because although strategies such as policing and public outreach are operational and amenable to short-term adjustments, changes in the design or rehabilitation of capital facilities to reflect security concerns are a longer term and more incremental enterprise. Accordingly, most respondents report that their agency intends to incorporate CPTED strategies into future facility designs.

Prior to 9/11, transit system security planning focused far more on personal and property crime than on acts of terrorism. Although efforts to address crime and terrorism are frequently complementary, they are not always one and the same. When asked how they tend to consider antiterrorism and anticrime strategies, most respondents reported viewing the strategies as either hand in hand (46%) or partly overlapping (41%). Across all agency types, only a few respondents, however, reported that anticrime and antiterrorism strategies were largely separate from one another.

POLICING STRATEGIES

Respondents were asked how policing is provided at their transit system. The survey instrument offered five potentially overlapping possibilities, plus an Other category:

- Sworn transit law enforcement (29%)
- Nonsworn transit police (i.e., private security) (53%)
- Contracted local police (28%)
- Dedicated bureau of local law enforcement (7%)
- No formal security, rely exclusively on local law enforcement (33%)

About one half (47%) of the agencies use just one policing strategy; this total includes 19% that have no formal security and rely exclusively on local law enforcement. The remaining agencies use a combination of policing options, with nonsworn transit police the most common. More than one half of agencies use nonsworn police for all (10%) or part (43%) of their policing activities. The least used policing option is a dedicated bureau of local law enforcement.

When comparing the 2002 USGAO survey results to our 2004 survey we found the percentage of systems relying on regular local law enforcement (33% in 2002 and 33% in 2004) or with a contracted or dedicated arrangement with local law enforcement (34% in 2002 and

35% in 2004) is essentially the same (USGAO, 2002). However, our 2004 survey found significantly higher shares of transit operators with an in-house transit police department of sworn officers (8% in the 2002 USGAO survey and 29% in our 2004 survey) and using nonsworn transit security (35% in 2002 and 53% in 2004). Although these differences might reflect random variation or bias in one or both of the two samples, the questions posed in these two surveys were similar enough to suggest that, in the 3 years since September 11, the proportion of transit agencies with in-house police and/or security services has increased significantly.

Systems with rail were more likely to rely on sworn transit police than systems without; 64% of agencies with rail used sworn transit police for at least one half of policing, compared to only 10% of agencies without rail. In contrast, systems without rail service were twice as likely to rely heavily on nonsworn police than were systems with rail (these differences are all statistically significant at the .05 level).

Ninety-two respondents provided us with information on the number of full-time equivalent security and/or police personnel contracted or employed by the agency. The numbers ranged from zero to 1,500 (at the Port Authority Trans-Hudson [PATH] headquartered in Jersey City, and with responsibilities for three airports and the New York seaports in addition to the PATH trains and stations). Sixteen agencies—all of which have rail—employ or contract more than 50 security personnel, and seven of these agencies have more than 100. More than one third of the agencies, however, reported having between 1 and 10 security personnel.

Regarding perceptions of effectiveness in addressing terrorist threats, policing strategies were ranked highest by respondents. Policing was ranked by 84% of respondents as "very" or "somewhat" effective in preparing for terrorist attacks. This percentage is higher (93%) for agencies with rail than without (81%).

SECURITY AND HARDWARE TECHNOLOGY STRATEGIES

In this era of rapidly evolving and extensively deployed information and communication technologies inside and outside the transit industry, it should come as no surprise that transit agencies are turning to technology to support increased security efforts. The most widely used security hardware technologies in the current sample were personnel radio communications systems, used extensively by more than 90% of all agencies—with rail and without. The only other technology hardware used extensively by more than one half the agencies is emergency alert and/or notification systems on transit vehicles, which are used by almost 70% of agencies. Public address systems and closed-circuit cameras are used to some degree by most agencies, while electronic access control, emergency telephones, and global positioning system (GPS) locators are used to some degree by about one half the agencies (see Figure 4). There was little use of the other security-related hardware and technologies asked about in our survey—such as tunnel intruder detection systems, explosives detection equipment, and chemical and/or biological sensors.

Owing to their more extensive control of rights of way and stations than bus-only systems, operators with rail are more than twice as likely to make extensive use of electronic access control and emergency telephones than systems without rail, and are somewhat more likely to make extensive use of public address systems, closed-circuit cameras, and GPS locators than systems without rail.

Just more than one fourth of the respondents consider security hardware strategies very effective in preparing for terrorist attacks, and an additional 55% think these strategies are somewhat effective—for a total of 81%. There is little difference of opinion on this type of strategy between respondents from systems with rail and those without rail.

PUBLIC EDUCATION AND USER OUTREACH STRATEGIES

A stream of crime and public safety literature has for years suggested that public awareness of and involvement in crime reporting and prevention can greatly increase the watchful "eyes

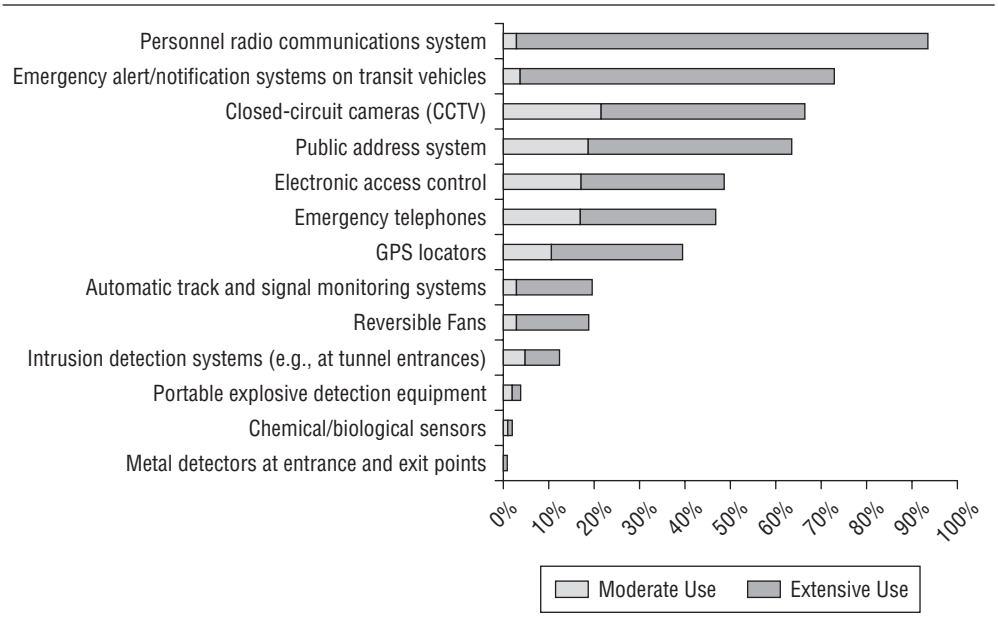

Figure 4: Security Hardware and/or Technology Strategies Employed by Agencies

on the street" and help to reduce the acceptability of petty and felonious criminal behavior (Jacobs, 1961; Newman, 1972). Many transit systems internationally—such as the London Underground—have for many years actively sought to enlist the help of patrons in watching for and reporting suspicious activity.

Efforts by transit agencies to educate passengers about safety and security issues appear to have increased dramatically since 9/11. In its 2002 survey, the USGAO found that just 18% of agencies surveyed had conducted transit safety and/or security campaigns prior to 9/11, whereas 23% had done so in the 6 months after 9/11. Two years later, our survey found a very different picture: 59% of agencies reported having a general emergency and safety education program in place, and 32% reported having programs specifically devoted to educating passengers about terrorism.

The proportion of surveyed agencies that have information and outreach strategies is significantly (at the .005 level) higher for those with rail than without. When asked about general emergency and safety programs, over three fourths of those from rail systems reported having such programs, and 67% have specific strategies to educate transit riders about dealing with terrorist attacks. Just over half of agencies without rail have established emergency and safety programs, and only 20% have terrorism-specific programs. In addition, nearly one third of respondents (30%) from agencies with rail reported having extensive programs in place to educate passengers about what to do in case of a terrorist attack, while none of the respondents from nonrail systems reported having such programs.

We found no differences between rail and nonrail agencies in the specific information and outreach strategies employed to educate transit riders about general emergency and safety issues and those strategies used to educate riders about dealing with terrorist attacks. Transit Watch programs are popular, as well as posters and pamphlets that emphasize the message that security is everyone's responsibility. Respondents also report using passenger newsletters, Web pages, public forums on transportation issues, and neighborhood outreach to keep riders informed.

Perceptions of the effectiveness of information and outreach strategies are more mixed, reflecting ambivalence about unduly alarming passengers.

Perceptions of the effectiveness of information and outreach strategies are more mixed, reflecting ambivalence about unduly alarming passengers. Just more than one half of all respondents consider such programs to be effective or very effective in preparing for terrorist attacks, though this percentage (71%) is higher for agencies with rail.

ENVIRONMENTAL DESIGN STRATEGIES

Although system design for transit security received little attention in the two previous security surveys of U.S. transit systems (Boyd & Sullivan, 1997; USGAO, 2002), this strategy was familiar to most respondents in our survey. More than two thirds (69%) of the respondents in our survey reported that they were familiar CPTED and could define the concept. And well more than one half (58%) of the respondents said that their systems employ CPTED strategies.

Given that rail transit systems tend to have many enclosed stations and miles of exclusive rights-of-way, it is not surprising that familiarity with and employment of CPTED strategies are higher at agencies operating rail transit service. Almost all of the respondents from agencies with rail (22 of 25, or 88%) indicated that they are familiar with CPTED and could define the concept. Seven of these 22 respondents from rail systems are associated with agencies that make extensive use of CPTED strategies, and the other 15 agencies reported having moderate CPTED strategy programs. By contrast, about one half (49%) of agencies without rail reported making use of CPTED strategies, and about two thirds (63%) of respondents from these agencies could define the term. Definitions of CPTED were reasonably consistent across respondents.

Two thirds of the respondents from the 61 agencies that make use of CPTED strategies think that these strategies are very important in overall security planning, whereas the remaining third considers CPTED strategies to be somewhat important to transit security efforts. No respondents considered the strategies to be unimportant. These perceptions were similar among systems with and without rail.

Figure 5 shows that agencies that use CPTED strategies are most likely to apply them to entrances and exits (82%), parking lots (75%), or gates (61%). By contrast, CPTED strategies are least likely to be applied to elevators, escalators, and vending machines. When asked to rank CPTED strategies that provide the most "bang for the buck," improved lighting and the addition of security cameras and/or closed-circuit TV were most commonly mentioned. Other strategies mentioned by multiple respondents were access control, open facility design with clear lines of sight, and landscaping.

When asked specifically about application of CPTED concepts to rail systems, about one half of the agencies with rail reported using CPTED in the design of maintenance facilities and station tunnels. The other components listed—control centers, traction power distribution centers, and tracks—were mentioned by between 20% and 40% of rail agency respondents.

Respondents from just 23 agencies reported having CPTED guidelines in place (10 with rail and 13 without) as of the summer of 2004; most (61%) of these guidelines were developed by an in-house team (14 of the 23 agencies with guidelines). Five contracted with consultants to prepare their CPTED guidelines, two used the sheriff's or police department's, and one developed guidelines through CPTED training at a local technical college. Only one operator reported using FTA security design guidelines at the time of the survey, though a few months after the survey, the FTA published a major report on transit security design considerations (Federal Transit Administration, 2004).

Conclusion

The findings of the current survey in many ways reflect the asymmetry inherent in U.S. public transit. Although hundreds of transit systems operate in many dozens of cities, most of the stations, vehicles, and passengers are concentrated on a few, very large, very high-profile systems—systems that are the most likely targets for terrorist attacks. The 10 largest U.S. transit systems (operating in nine metropolitan areas) carried 65% of all transit trips reported to the FTA for 2002, whereas the remaining transit systems carry the other 35%. Of all 2002 U.S. transit trips, 39% occurred in one metropolitan area, New York, and 31% of all U.S. transit trips were carried by just one system, the New York Metropolitan Transportation Authority (MTA) (American Public Transportation Association, 2004).

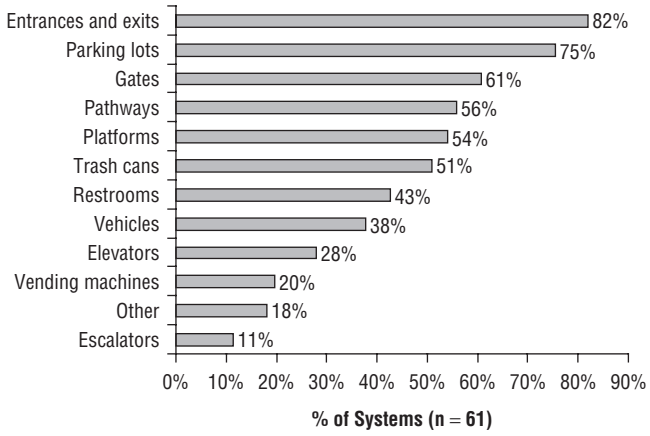

Figure 5: Components for Which CPTED Strategies Are Used
NOTE: CPTED = crime prevention through environmental design.

Although significant attacks against U.S. transit systems remain rare, they are likewise asymmetric. Just 16 of the 80 systems with rail service and/or enclosed bus or ferry terminals queried for this research reported receiving a credible threat (e.g., bomb, chemical, biological, fire attacks) between the summer of 2003 and the summer of 2004. Although 14 of these 16 systems had received fewer than five threats, one agency reported receiving 12 credible threats, and the other reported receiving 31. These threats and incidents, combined with the tragic events of September 11 and the more recent, deadly transit attacks in Spain and London, have pushed security to the forefront of transit policy debates.

This survey of 113 U.S. transit systems finds that attention to transit system security increased significantly after 9/11, owing to increased public and political attention to the issue, and more specifically to federal and transit industry initiatives. This increased attention was translated in the 3 years after 9/11 into the increased use of policing, security technology, public information and outreach, and CPTED strategies. In its 2002 survey of U.S. transit systems, the USGAO found that just more than half (54%) of transit systems had conducted security threat assessments. Just 2 years later, we found that the proportion of large U.S. transit agencies that had conducted such assessments had increased to 85%.

Our survey asked in detail about four types of security strategies: policing, technology, education and outreach, and environmental design. We found that attention to all of these strategies has increased since 9/11, and more than one half of the respondents now view all four strategies as central or significant parts of security planning efforts. Prior to 9/11, CPTED and, especially, education and outreach were given much less weight in security planning by the respondents to our survey. Because they manage and operate large numbers of stations and rail rights-of-way, respondents from rail transit systems tended to exhibit higher levels of advanced planning on security issues than did respondents from systems with no rail service.

More than 80% of the respondents to our questions on system design now believe that CPTED is a somewhat or very effective strategy in preventing terrorist attacks. This ranking of effectiveness is similar to policing and security hardware and technology strategies (though we should note that one half again as many respondents answered questions about policing and technology as those who answered questions about CPTED strategies). Among the four types of security strategies analyzed here, public education and user outreach strategies were generally viewed as less effective than the other three types of strategies; nonetheless, 58% of respondents rated these strategies as somewhat or very effective. In general, systems with rail were more likely to view most strategies as very effective as compared to systems without rail.

Collectively, the findings of the current survey reflect the fundamental dilemmas of transit security planning. On one hand, the time, energy, and resources devoted to transit system security have increased dramatically during the past decade, particularly since September 11, and a majority of respondents to this survey view the four distinct security strategies as either somewhat or very effective in increasing transit safety and security: policing (84%), technology (81%), education and outreach (58%), and system design (82%). On the other hand, because they are inherently open, dynamic systems that congregate hundreds, and even thousands, of people together in stations and onto vehicles, most transit managers and security officials responding to our survey continue to view transit systems (with the exception of paratransit services) as very vulnerable to terrorist attacks.

Note

1. In July 2004, the name of the U.S. General Accounting Office was changed to the U.S. Government Accountability Office.

References

American Public Transportation Association. (2004). *Transit agency data*. Retrieved November 2004, from www.apta.com/research/stats/

Boyd, A., & Sullivan, J. P. (1997). *Emergency preparedness for transit terrorism*. Washington, DC: National Research Council.

Federal Transit Administration. (2004). *Transit security design considerations* (No. FTA-TRI-MA-26 7085-05, DOT-VNTSC-FTA-05-02). Washington, DC: Federal Transit Administration Office of Research Demonstration and Innovation, Office of Program Management, U.S. Department of Transportation.

Jacobs, J. (1961). *The death and life of great American cities*. New York: Random House.

Jenkins, B. M. (1997). *Protecting surface transportation systems and patrons from terrorist activities: Case studies of best security practices and a chronology of attacks* (No. IISTPS Report 97-4). San Jose, CA: Norman Y. Mineta International Institute for Surface Transportation Policy Studies.

Jenkins, B. M., & Gersten, L. N. (2001). *Protecting surface transportation against terrorism and serious crime: Continuing research on best security practices* (No. Report 01-07). San Jose, CA: Norman Y. Mineta International Institute for Surface Transportation Policy Studies.

Newman, O. (1972). *Defensible space*. New York: Macmillan.

Singleton, R., Straits, B. C., Straits, M. M., & McAllister, R. J. (1988). Measurement. In *Approaches to social research* (pp. 97-129). New York: Oxford University Press.

U.S. General Accounting Office. (2002). *Mass transit: Federal action could help transit agencies address security challenges* (No. GAO-03-263). Washington, DC: Author.

Yin, R. K. (2003). Case study research design and methods. In *Applied social research methods* (3rd ed., Vol. 5, pp. 1-18). Thousand Oaks, CA: Sage.