

This piece was published before the May 2007 rebranding of Mercer Management Consulting, Mercer Oliver Wyman, and Mercer Delta Consulting as **Oliver Wyman**.

Oliver Wyman

Oliver Wyman is building the leading global management consultancy, combining deep industry knowledge with specialized expertise in strategy, operations, risk management, organizational transformation, and leadership development. The firm works with clients across a range of industries to deliver sustained shareholder value growth. We help managers to anticipate changes in customer priorities and the competitive environment, and then design their businesses, improve their operations and risk profile, and accelerate their organizational performance to seize the most attractive opportunities.

www.oliverwyman.com



MARSH MERCER KROLL
GUY CARPENTER OLIVER WYMAN

Rail Transit and the Security Challenge

By Gilles Roucolle and Rick Lowes

Passenger railroads and public transit systems¹ have long faced a range of security issues, from ensuring passenger safety to preventing equipment damage and theft. Escalating terrorist attacks over the past decade have only added to this security challenge: From 1998 to 2003, there were 181 terrorist attacks on trains and rail-related targets (such as stations) worldwide, resulting in 431 deaths.² But it has taken more recent large-scale attacks, such as on the Moscow and London metro systems and the Madrid regional passenger rail system, which claimed another 288 lives, to raise concerns about rail safety to new levels. These concerns have been reflected in increasing press coverage and policy discussions, the introduction of new anti-terrorist laws in some EU countries, and recent studies on passenger rail and transit security issued by the US Government Accountability Office.

Despite worries over rail and public transit safety, however, improvements in rail-related security have been slow to emerge, driven partly by low levels of transit authority investment and partly by the complexity of the challenge. The good news is that recent renewed R&D for security technologies and the emergence of a more diversified base of security solutions providers is improving the potential for feasible, cost-effective rail security solutions. In particular, the development of integrated “bundled” options (that combine security, safety, communications, and other services) should both simplify the process and improve the outcomes of security-related investments.

The Investment Dilemma

Recent attacks on rail and transit systems have been horrific and truly felt round the world. Yet broad-based investment in rail security remains low, for several reasons. Passenger rail systems in many countries face continuing financial pressure, caught between limited income from the farebox and subsidies on the one hand and the need to upgrade critical infrastructure and equipment on the other. Thus incremental investments, such as security upgrades, are unlikely to be funded internally unless specifically mandated. Moreover, the relatively infrequent and localized nature of rail terrorist attacks makes proactive investment in rail difficult to justify from a return on investment perspective.

Governments have not exactly “stepped up” in terms of supporting rail on par with other threatened economic sectors. Some governments did provide increased funding after 9/11 and recent rail attacks, but the overall level of support remains low—certainly vastly lower than spending on aviation on a per passenger basis. As an example, the US federal government annually spends more than \$8 per passenger for investments related to air travel security and one cent per passenger to ensure the safety of the nation’s public transit systems.³

¹ Includes intercity rail, heavy and light commuter rail, and metropolitan transit systems.

² RAND Corporation and the Oklahoma City Memorial Institute to Prevent Terrorism.

³ *Transfer*, Surface Transportation Policy Project.

At present, an “attack then invest” mentality seems to predominate: The EU stepped up funding following rail attacks there (including \$320 million for security research), but the US federal government may actually reduce funding on transit, passenger, and freight rail security—from \$150 million in FY2005 to \$100 million in FY2006.⁴ Meanwhile, US transit agencies are reporting an outstanding need for more than \$6 billion in security-related investments.⁵

A lack of proactive investment in rail security, however, is terribly shortsighted. Although the risk of a terrorist attack on any one system is low, such an attack will accomplish the perpetrators’ intent—not only to harm civilians and cause terror in the short term but to damage a region’s economy over the longer term. As an example, the July 7, 2005 London bombings cost an estimated \$1.08 billion in lost tourism and transport revenues, and passenger numbers only recovered to 2004 levels after three months. Operational costs increased permanently by 10 percent for additional safety and security measures. The ongoing cost for policing and security for the London Underground is estimated to be about \$115 million annually. In New York City, damage to the subway system on September 11, 2001 generated an estimated \$531 million in losses (including rescue and recovery expenses, lost fares, and tax reduction) and a massive injection of \$1.1 billion in capital was required for transit system rebuilding and security improvements.

The Implementation Challenge

If the money can be found to improve the security of a rail or public transit system, there is still the problem of ensuring such investments are effective—that is, that they actually improve the security of the overall system in terms of thwarting attacks and enhancing passenger safety. Transit systems are highly complex: for example, the London Underground has 275 stations, 253 miles of track, and serves 2.7 million passengers per day. This raises many challenges to the implementation of effective security measures:

- Passenger stations: How to effectively screen large numbers of passengers without disrupting on-time performance, reducing service frequencies, and diminishing the customer appeal of rail?
- Vehicles and wayside: How to provide effective security where vehicles make frequent, open stops?
- Rail trackage: How best to protect an asset that is highly vulnerable at any point over dozens or hundreds of miles?

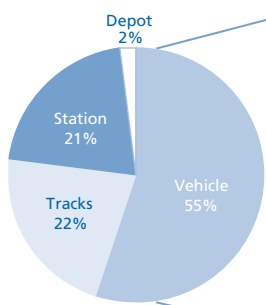
As shown in Exhibit 1, all of these areas are vulnerable to attack. Determining the best way to secure each one is not a problem that can be solved easily, but several emerging factors point to the potential for near-term enhancement of the effectiveness of rail security solutions: a broadening base of tech-savvy and competitive suppliers, a host of cutting-edge technologies, and the development of truly integrated security solutions.

⁴ CRS Report for Congress: Passenger Rail Security: Overview of Issues.

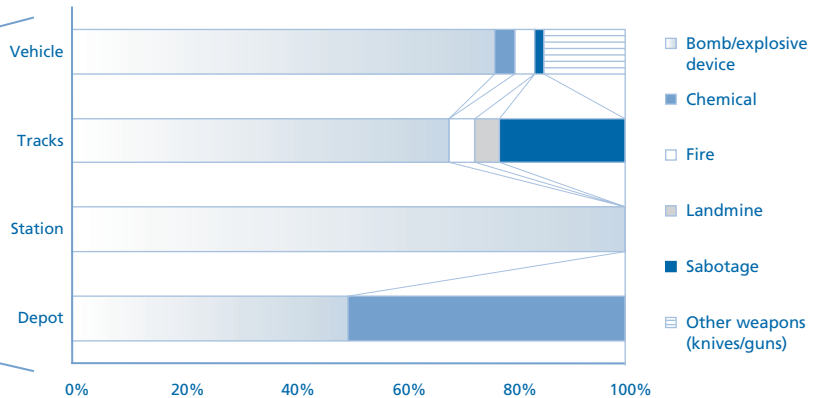
⁵ Survey of US Transit System Security Needs and Funding Priorities, American Public Transport Association, April 2004.

Exhibit 1 Attacks on Rail Systems: Locations and Tactics, 1997-2004

Incident Location: 1997-2004
(% of total rail incidents)



Tactics Used in Rail Incidents: 1997-2004
(% of total rail incidents)



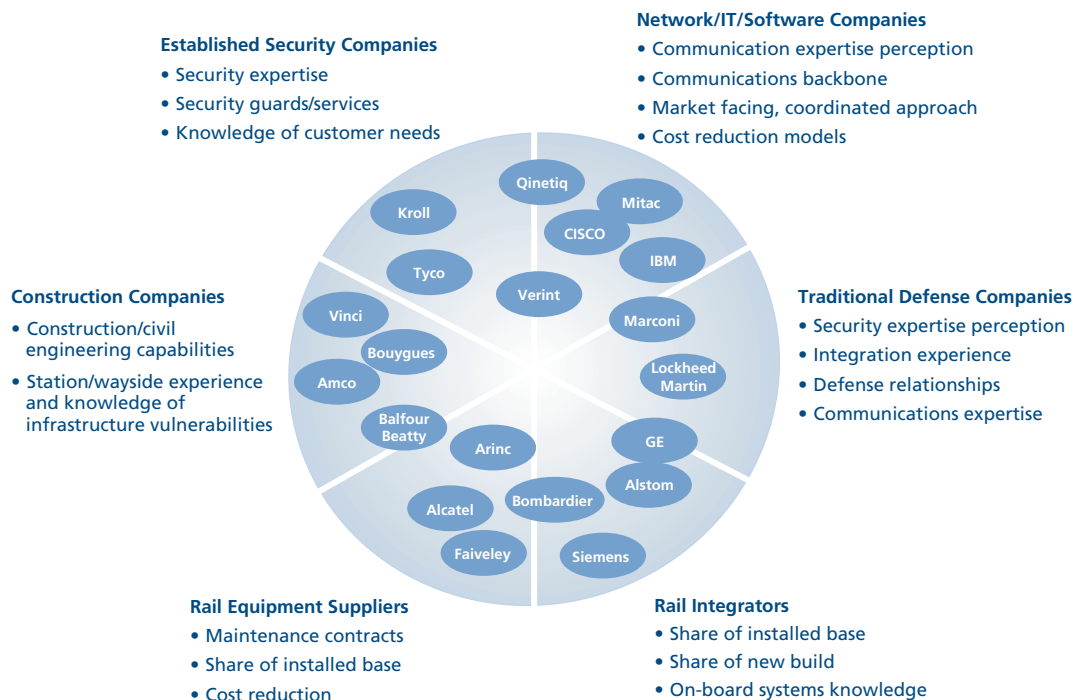
Source: US Department of Transportation, Memorial Institute of Terrorism Knowledge, Mineta Institute of Transportation.

A Broader Supplier Base

Traditional security solutions providers, such as Siemens and Tyco, are being joined by a range of diverse players, heating up the competitive intensity of the market. Sectors that are showing new interest in rail security include defense contractors, rail equipment suppliers and integrators, network/IT companies, and construction companies.

These businesses can pull different levers to position themselves as potential competitors in the rail security space (Exhibit 2). But the overall positive impact of this broadening supplier base is that it will drive R&D spending and the development of increasingly better solutions to meet a wider range of rail and transit system security needs.

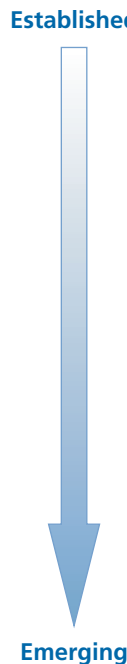
Exhibit 2 Emerging and Potential Rail Security Solutions Providers



Enhanced Technology Options

Traditional security technologies, such as analog closed-circuit television (CCTV), with either control center monitoring or locomotive engineer monitoring, require constant human attention and have proven to be only moderately effective. Newer technologies take advantage of computing power and automation to massively increase the quality and quantity of information that can be processed. A range of potential technologies are shown in Exhibit 3—some of these are available today, while others will require further research and refinement. “Intelligent” CCTV and blast containment are likely to be the first technologies to be implemented widely.

Exhibit 3 **Potential Rail Security Technologies**



Technology	Current Status
Digital CCTV with high-speed wireless monitoring	Highly desirable: deters both terrorism and crime, provides visual evidence, can facilitate immediate response to threats
Blast containment	Stations and cars can be built or retrofitted with containment measures to reduce the severity of attacks
Audio detection	Allows for quick identification of gunshots, can alert personnel in the event of shouting/screaming
Facial recognition	Can be linked to police/government databases
Object detection	Can identify motionless "high risk" objects on cars (and eventually on tracks)
Milimeter wave detection	Could potentially replace today's x-ray technology; trials underway in London and New York
Chemical, biological, and explosive agent detection	Could have potential for use in stations

Integrated Solutions

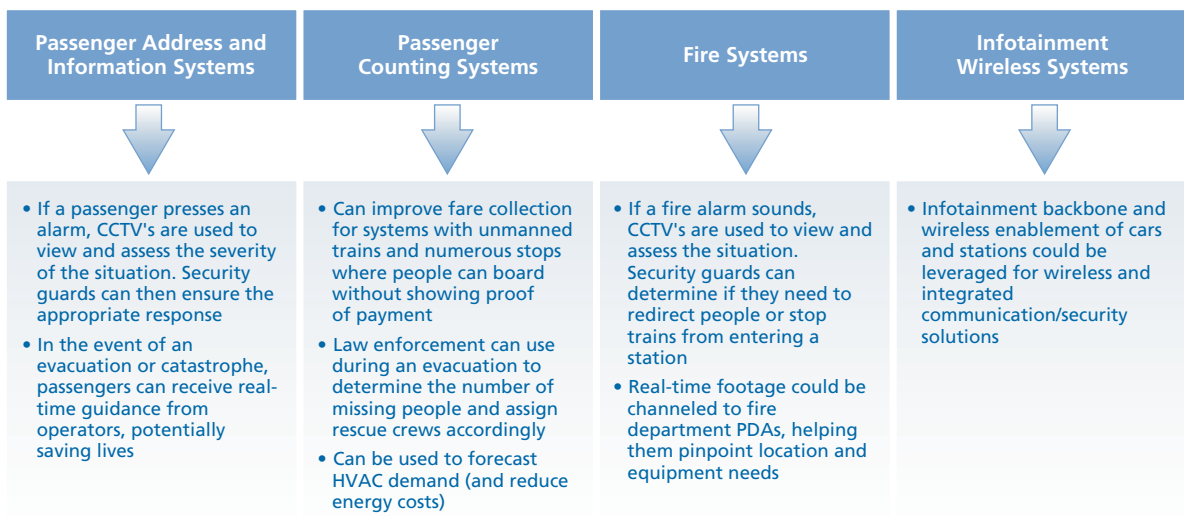
Most critically, some rail suppliers are now focusing on how they can provide needed security technologies for the rail or public transit system as part of a “bundled” or integrated rail solution—one that ties together safety, security, communications, and rail control systems. Given the proliferation of new security technologies, implementing such a bundled solution could enable operators to reduce the costs and risks involved in choosing and assembling off the shelf technology themselves.

Moreover, some of these new integrated solutions will offer step changes in security effectiveness. Automatic control of a train based on security issue detection, for example, would minimize personnel-driven delays and the risk of a deadly train entering a highly populated terminal. Let alone providing the ability to detect and prevent attacks, integrating a rail provider’s security

systems with police/emergency response teams would enable a virtually immediate response, while emergency teams would have access to critical event information via wireless CCTV's and remote monitoring.

Beyond addressing security issues, some of these new integrated systems could even provide access to previously untapped value. Operating costs could be reduced by automating certain personnel-based monitoring functions, for example, while using an improved communication infrastructure to bundle infotainment services and wireless access for customers could provide new revenue streams (Exhibit 4).

Exhibit 4 **Potential Multi-Use Rail Systems Integration Scenarios**



Ensuring the Future of Rail Transit

Proactive investment in rail security may help railroads and public transit systems not only avoid significant losses by preventing future attacks but also, more immediately and tangibly, maintain or reduce security-impacted operating costs. Given available new technologies and the growing interest of rail suppliers and other security-oriented firms, solutions that involve less risk and that could potentially generate incremental value are becoming increasingly feasible. As some have already realized, rail operators should not need to wait for new laws or the next attack to begin focusing on opportunities to better protect themselves and their passengers.