TRANSPORTATION RISK MANAGEMENT: A NEW PARADIGM

Mark D. Abkowitz, Ph.D.
Professor of Civil Engineering
Vanderbilt University
Box 1831, Station B
Nashville, TN 37235
615/343-3436 (phone)
615/322-3365 (fax)
Mark.Abkowitz@Vanderbilt.edu

July 2002

Submitted for consideration for presentation at the Annual Meeting of the Transportation Research Board and for publication in *Transportation Research Record*

word count = 4,750

TRANSPORTATION RISK MANAGEMENT: A NEW PARADIGM

Mark D. Abkowitz, Ph.D.
Professor of Civil Engineering
Vanderbilt University
Box 1831, Station B
Nashville, TN 37235
615/343-3436 (phone)
615/322-3365 (fax)
Mark.Abkowitz@Vanderbilt.edu

ABSTRACT

Over the past decade, risk management has been evolving into a core business practice in government and industry. In the transportation sector, the overarching risk management objective has been to reduce accident likelihood and severity. Where hazardous materials shipments are involved, this extends to spill prevention and mitigating the consequences when a release occurs.

Until recently, the approach to transportation risk management assumed that when man-made disasters occurred, they were accidental in nature and not due to malicious intent. Terrorist activities, culminating with the tragic events of September 11, 2001, have dramatically changed this landscape. In particular, we have learned that assessment of transportation risk must be performed with a more expanded scope to accommodate terrorism scenarios that heretofore would have been considered so unlikely that they did not warrant risk management attention. Similarly, emergency responders must be able to handle impacts far beyond what was previously imaginable in terms of number of victims, deployment of response resources and agency coordination.

Given these circumstances, it is apparent that decision-makers need to employ a new paradigm for transportation risk management. In particular, this paradigm must: 1) more explicitly consider security threat and vulnerability, and 2) integrate security considerations into the overall framework for addressing natural and man-made disasters, be they accidental or planned. This paper introduces this paradigm and recommends actions that will enable security considerations to become an integral part of transportation risk management.

INTRODUCTION

Over the past decade, risk management has been evolving into a core business practice in government and industry. In the transportation sector, the overarching risk management objective has been to reduce accident likelihood and severity. Where hazardous materials shipments are involved, this mission extends to spill prevention and mitigating the consequences when a release occurs.

Until recently, the approach to transportation risk management assumed that when man-made disasters occurred, they were accidental in nature and not due to malicious intent. Terrorist activities, culminating with the tragic events of September 11, 2001, have dramatically changed this landscape. In particular, we have learned that assessment of transportation risk must be performed with a more expanded scope to accommodate terrorism scenarios that heretofore would have been considered so unlikely that they did not warrant risk management attention. Similarly, emergency responders must be able to handle impacts far beyond what was previously imaginable in terms of number of victims, deployment of response resources and agency coordination.

Given these circumstances, it is apparent that decision-makers need to employ a new paradigm for transportation risk management. In particular, this paradigm must: 1) more explicitly consider security threat and vulnerability, and 2) integrate security considerations into the overall framework for addressing natural and man-made disasters, be they accidental or planned.

It is important to recognize that transportation security and traditional risk management share a common objective:

> *To reduce the likelihood and consequences of disasters so as to protect human health, quality of life and the environment.*

As a result, an opportunity exists for security considerations to be folded into an overall decision-making framework that guides how risks are assessed and where resources are allocated so as to generate the best "return on investment". The process can then be governed by addressing a fundamental set of risk management questions (see Figure 1).

The purpose of this paper is to: 1) review traditional transportation risk management methods and practices, 2) introduce security issues into this framework and 3) recommend actions that enable security considerations to become an integral part of transportation risk management. This "big picture" conceptual view could serve as a catalyst in the development of an agenda that will enable transportation risk managers to devote resources where the overall impact is most beneficial, be it through enhanced security or by implementing other risk management control strategies.

THE RISK MANAGEMENT SPECTRUM

Traditionally, risk management has focused on two primary causes of concern, natural and man-made disasters. Natural disasters include a wide range of events, such as floods, earthquakes, forest fires, tornados, hurricanes, and avalanches. The prevailing attitude has been that these events are "acts of God" and there are limitations on what one can do to prevent incident occurrence. Consequently, the majority of risk management attention in these circumstances has been focused on mitigating the consequences of these incidents when they do occur.

Man-made disasters pose a different problem, both in terms of risk tolerance and the focus of risk management attention. Whether due to human error, poor design or faulty technology, man-made disasters are associated with the failure on the part of an individual or

organization to make the appropriate decisions that adequately protect human health, property and the environment. Hence, society's risk tolerance for man-made events is much lower than for natural disasters and there is greater public scrutiny applied to how these risks are managed. Moreover, since the event is man-made, risk management attention and resources are devoted to both incident prevention and mitigating the consequences of the incident should it occur.

Whereas, traditionally man-made disasters have been considered largely accidental in nature, the events of September 11, 2001 underscore the significance of intentional acts of terrorism as both a leading cause of incidents as well as creating the potential for more significant consequences. As shown in Figure 2, the new transportation risk management paradigm needs to explicitly accommodate this additional source of causation and wider range of potential consequence.

In addition, we have learned that acts of terrorism can target new pathways. Historically, attention has been focused on chemical/nuclear incidents, leading to fire/explosion and/or toxic release. New scenarios now require formal recognition, such as bio-terrorism and cyber-terrorism [1], as well as physical attack where large groups are congregating (e.g., congested traffic areas, parade routes). Moreover, many believe that use of biological agents and computer viruses threatens a larger population in ways that our science and technology cannot fully comprehend, raising the level of public anxiety that much more.

RISK ASSESSMENT

Risk assessment focuses on the ability to measure the likelihood of a potential event and its associated consequences. The introduction of man-made disasters caused by malicious intent into the risk management spectrum suggests a need to re-visit traditional approaches to determining likelihood and consequence. In the discussion below, consequence measurement is addressed first.

When an incident takes place, the consequences can range from no impact to what is typically referred to as a "worst-case scenario". A worst-case scenario, although considered an extremely unlikely event, characterizes what is believed to be the most catastrophic result imaginable given the incident circumstances. Traditionally, most worst-case scenarios have involved predictions of multiple fatalities and injuries, but rarely, if ever, have they considered consequences of the scale witnessed at the World Trade Center, simply because it was beyond what risk managers considered plausible. Under a new paradigm, a broader set of consequences with more far-reaching effects must be actively considered. This, in effect, extends the consequence scenario range, as shown in Figure 3.

To more effectively measure overall impact, a new approach to evaluating consequences is also recommended, one that takes into consideration a more comprehensive account of contingent and societal effects. Meaningful impact measures include:

- Fatalities & injuries (acute and long-term)
- Cleanup & disposal costs
- Property & product damage
- Loss due to business interruption
- Environmental degradation & ecosystem damage
- Traffic & community disruption
- Public anxiety
- Diminished agency/company value and image

The obvious benefit of a more accurate measure of consequence is the ability of transportation risk managers to make more informed decisions.

Paradigm changes are also needed in determining incident likelihood. The altering effects of September 11, 2001 on incident likelihood are shown in Figure 4. With a new catalyst for incident occurrence and the potential for far greater consequences than previously imagined, incident likelihood can be expected to increase somewhat across the entire range of potential consequences, with the consequence range having been extended to include more catastrophic scenarios.

Putting these risk assessment concepts into practice poses a challenge due to the limited history of terrorist acts from which to estimate event probabilities and predict consequences. Overcoming this impediment will require extensive use of what can be inferred from empirical data combined with the development of predictive models based on the theory of scenario structuring and logical inference [2].

PRIORITIZING TRANSPORTATION RISK

Despite public outcry for a completely safe world, resource constraints (e.g., people, time, money) will always exist that preclude such a goal from being fully achievable. Hence, the risk management process must be oriented towards the prioritization of risks, prompting those of greatest concern to become the focus of improved control.

Risk prioritization and follow-through is a process-oriented activity, involving the following steps: 1) identify critical transportation facilities, 2) perform risk assessments, 3) develop risk management control strategies (prevention & deterrence; preparedness; response; recovery), 4) implement control strategies and 5) monitor performance [3].

While perhaps simple in concept, successful implementation of this process within the transportation sector is an ambitious task. Our nation's transportation infrastructure is large and diverse, representing a variety of potential terrorist targets. This infrastructure, supporting both passenger and freight transportation, contains:

- Highways
- Pipelines
- Railroads
- Navigable waterways
- Air transport networks
- Fixed facilities (traffic management centers, terminals, transfer and storage sites, rest areas)
- Infrastructure hot spots (e.g., bridges, tunnels)
- "Vehicles" that use these facilities

Whether conducted on a local, state or national scale, it will be important for the risk prioritization process to be inclusive by involving all relevant parties in the region of interest. This will help ensure that all potential transportation vulnerability points have been identified and evaluated at the front end of the process, allowing risk management priorities and control strategies to be determined with the confidence of knowing that a systematic process was used in making these decisions.

INSTITUTIONAL COORDINATION AND DECISION-SUPPORT

Risk management embodies risk communication (sharing information) in addition to risk assessment (generating information). Within the transportation industry, there are a variety of

influential parties who, in effect, operate as risk managers (see Figure 5). In the public sector, this can include a multitude of federal, state and local agencies [4]:

Federal Government

- Department of Transportation
- Environmental Protection Agency
- Federal Emergency Management Agency
- Department of Defense
- Department of Energy
- Department of Justice

State Agencies

- Emergency Management
- Transportation
- Environmental Management
- Law Enforcement
- Public Safety
- Health Departments

Local Government

- Emergency Operations Centers
- Local Emergency Planning Commissions
- Port, Bridge and Tunnel Authorities
- Fire Departments
- Local Police
- Water Departments
- City Planners

Because there are multiple stakeholders involved, it has always been important to understand the circumstances under which each party has jurisdiction, the need for mutual agreements and the upward compatibility (i.e., local to state to federal) of emergency preparedness.

The introduction of security risk exacerbates this situation, however. First, the need for timely and accurate, yet secure, information is even more compelling. Secondly, a large number of risk managers are likely to be involved, resulting in an increase in the scale and type of communication interfaces that must be established and maintained. Finally, the magnitude of potential consequence requires these parties to prepare for managing and deploying greater response resources to more victims over a larger geographical area.

ENABLING TOOLS

To meet these expectations, transportation risk managers will be asked to handle a variety of responsibilities, such as being able to:

- Plan & track before/during/after a major event
- Assess & prioritize locations in need of risk management attention
- Identify at-risk populations & sensitive environments
- Communicate risks to affected parties
- Locate & deploy response resources
- Estimate damage
- Identify & evaluate mitigation strategies
- Maintain a centralized risk management information system

The availability and use of a variety of enabling tools will be critical in supporting these needs. Several of these tools are discussed below.

Knowledge and Awareness Building
An important part of the transition into a new paradigm is to be able to share the vision and concept with transportation risk managers in a nurturing environment. This provides the opportunity to introduce new ideas as well as to invite feedback. Through channels such as conferences, workshops, training courses, guidebooks and web sites, knowledge and awareness building can be provided in a manner consistent with a transportation risk manager's ability to absorb information and adapt to change.

Process Development
A systematic approach to identifying critical transportation facilities, performing risk assessments, implementing risk management control strategies and monitoring performance requires the development of policies and procedures to guide the process. Activity flow diagrams should be created that identify all possible transportation infrastructure that could be subject to natural and man-made (accidental and intentional) risks. Credible methods and practices should be established for assessing and prioritizing these risks as well as evaluating and selecting management control strategies. Finally, meaningful measures of risk management performance should be defined along with appropriate data collection mechanisms. Within each of these process steps, key stakeholders should be identified and tasks assigned, so that accountability can be established and monitored.

Intelligence Gathering
The effectiveness of the transportation risk management process will be strongly influenced by the quality of the information used in its execution. Determining threat and vulnerability requires access to information that enables the transportation risk manager to define the range of consequence scenarios and assign corresponding likelihood. Although some of this information may be available either in the public domain or resident within the organization, liaison with the intelligence community will likely improve data quality in terms of information breadth, depth and accuracy.

Emergency Response Planning
With an expanded set of consequences to consider and the potential for more severe impact, the preparedness community should re-consider its approach to emergency response planning. At the outset, it may be desirable for the region of interest to identify: 1) all the transportation risk managers that might be involved in an emergency response, 2) the coordination & communication links that presently exist between respective organizations, 3) how well these links are performing and 4) other communication & coordination links that need to be established. Based on these findings, a regional response plan can emerge in which any anticipated transportation risk with significant potential for harm will have been pre-screened, with the deployment and management of the response activity carefully laid out. With this structure in place, preparedness exercises (e.g., simulated emergencies) can be devised that offer greater benefit to the region because emphasis can be placed on more critical concerns and involve the appropriate risk managers.

Information Management

At the crux of any transportation risk management activity is the ability to obtain, store, analyze and share information [5]. Because transportation involves both static (e.g., location of fixed facility) and dynamic (e.g., location of rolling stock) operations, a variety of technologies offer the potential to support risk management information needs. These include:

- Surveillance and detection technologies (e.g., remote sensing, electronic tags)
- Geographic information systems (GIS)
- Global positioning systems (GPS)
- Communications devices and networks

As a case in point, we are beginning to see the proliferation of software applications that utilize GIS to provide visual maps of risk scenarios, showing the location of exposed population as well as proximity to emergency response resources. These images and underlying data can be updated by GPS field devices and served via the Internet, call-out systems and other communication technologies to broadcast information to both internal and external audiences. A key to progress in this domain will be to harness only those aspects of available technology that result in practical, easy-to-use tools that enable transportation risk managers to perform their duties with a high degree of confidence.

A WORD OF CAUTION

Considerable attention and resources are currently being allocated to security initiatives in response to the events of September 11, 2001. While it became painfully evident that enhancing security is an immediate risk management priority, it is nonetheless important to understand the long-term ramifications of devoting a disproportionate amount of resources to enhanced security. This holds particularly true if security resources are drawn from a general pool of funds allocated for risk management activities.

The ultimate concern is that while there may be a high return on investment by flowing resources into controlling security risk in the short-term, eventually a point of diminishing return will be reached, where the next increment of security risk investment will not produce an attractive risk benefit. A disproportionate allocation of funds directed at security risk also implies a shift of resources away from managing accidental man-made and natural disaster risks. Deferring investment in new and ongoing control strategies in these areas for an extended period time could leave society overall more vulnerable to the risk.

Figure 6 illustrates this tradeoff by showing the potential impact of investing in security risk initiatives versus other risk management strategies. Investment in security initiatives may be strongly advisable now because of the risk benefits that can be achieved (point A). As diminishing returns are realized over time, reaching a point where new investment in managing non-security risks will produce greater societal benefit than continued investment in security risk (point B), the value in shifting resources to other risk management initiatives will become apparent. Ultimately, a balance of investment in security risk and other transportation risks (point C) will represent the most effective use of transportation risk management resources.

Knowing when point B has been reached and being agile in adjusting risk management resource investment to reach point C would be exceedingly difficult if security risks are managed in a separate “silo” from traditional risk management activities. If security and traditional risk management activities were evaluated, controlled and monitored as part of a single, integrated function, then undesirable risk management results could be avoided.

This argument also applies to risk communication considerations. For example, there is a growing debate over how to manage the delicate balancing act between the public's right-to-know and making potential targets less transparent to terrorists. A case in point is EPA's Clean Air Act, Risk Management Plan (RMP) rule. This rule requires thousands of industrial facilities, mostly chemical plants, to prepare and submit documentation describing the worst-case scenario incident that could occur at the facility. Were this information to be made publicly available, as initially planned, a terrorist contemplating an act of malicious intent could easily assemble a prioritized list of potential targets [6]. While a decision not to make RMP submittals accessible to the public could be an effective short-term deterrence strategy, continued restrictions on the availability of this information could eventually create greater societal risk, because the communities in proximity to these facilities would lack valuable information from which to improve emergency preparedness in the event of an industrial accident.

SUMMARY

The visibility of terrorist activities has prompted us to re-think how to effectively manage the risks associated with our nation's transportation infrastructure. This paper suggests that a new transportation risk management paradigm is needed to accommodate considerations associated with assessing and communicating the risks of man-made disasters caused by intentional acts.

Because of the added complexities associated with managing security risks, institutional coordination and decision-support becomes even more critical. As transportation risk managers will be expected to handle a variety of responsibilities, the availability and use of enabling tools will be essential. These tools include knowledge and awareness building, process development, intelligence gathering, emergency response planning and information management. Information technology will play an important role in this regard, provided that technology is utilized to develop practical, easy-to-use tools that enable transportation risk managers to perform their duties with a high degree of confidence.

The significance of integrating security risk with other transportation risks should not be underestimated. As opposed to these risks being managed in separate silos, if they are evaluated, controlled and monitored as a single, integrated function, better overall risk management strategies will emerge and the likelihood of producing undesirable risk management results can be avoided. The net result is the best protection we can provide society with the means that are available.

REFERENCES

1. Morgan, D. F. and H. N. Abramson, "Improving Surface Transportation Security Through Research and Development", TR News, No. 211, November/December 2000, pp. 28-30.

2. Garrick, B. J. "The Conceptual and Philosophical Basis of Quantitative Risk Assessment", presented at the Frank L. Parker Distinguished Lecture Series, Vanderbilt University, Nashville, November 2001.

3. Chin, S. M., H. L. Hwang, O. Franzese and L. D. Han, "Security Vulnerability Assessment Resources for U.S. Highway Network", presented at the Annual Meeting of the Transportation Research Board, Washington, January 2002.

4. AASHTO, “Security and Emergency Response Survey of State Transportation Agencies”, presented at the Annual Meeting of the Transportation Research Board, Washington, January 2002.

5. Flynn, S. E., “Transportation Security Agenda for the 21st Century”, TR News, No. 211, November/December 2000, pp. 3-7.

6. Willis Environmental, “Evaluation and Prioritization of the Environmental Risks of Terrorist Action”, November 2001.

LIST OF FIGURES

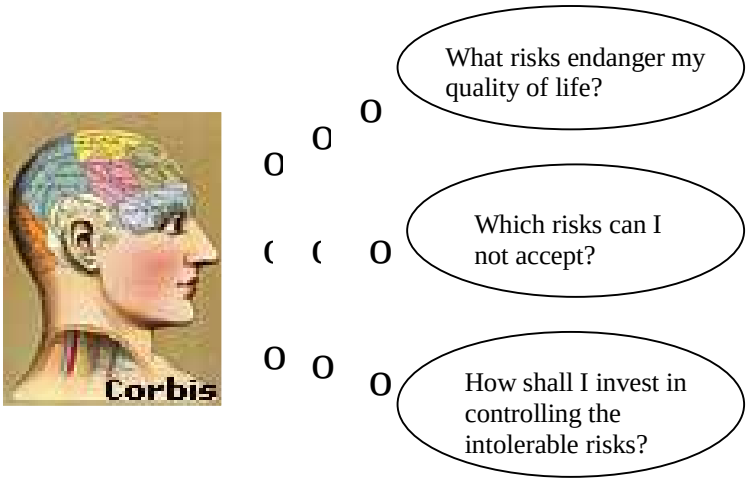

FIGURE 1 Fundamental risk management questions.

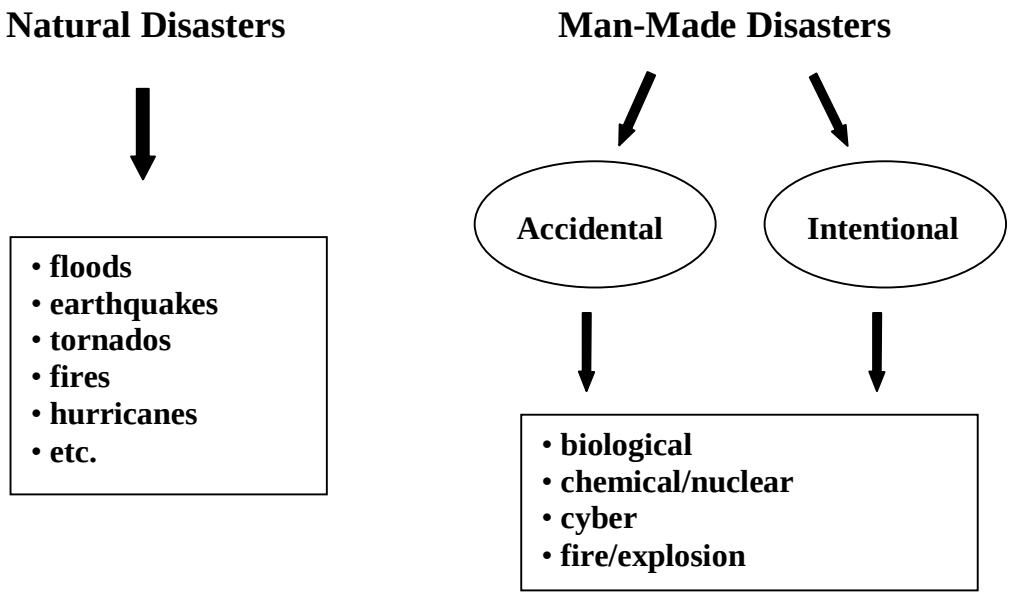

FIGURE 2 The risk management spectrum.

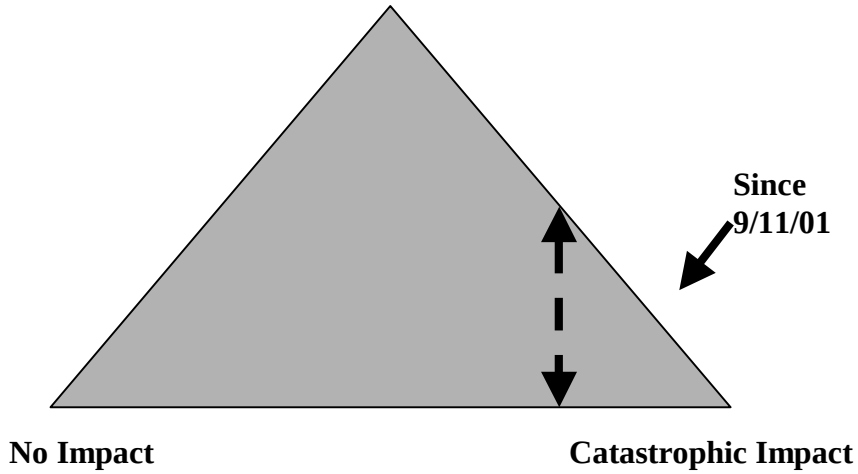

FIGURE 3 Re-visiting consequence scenarios.

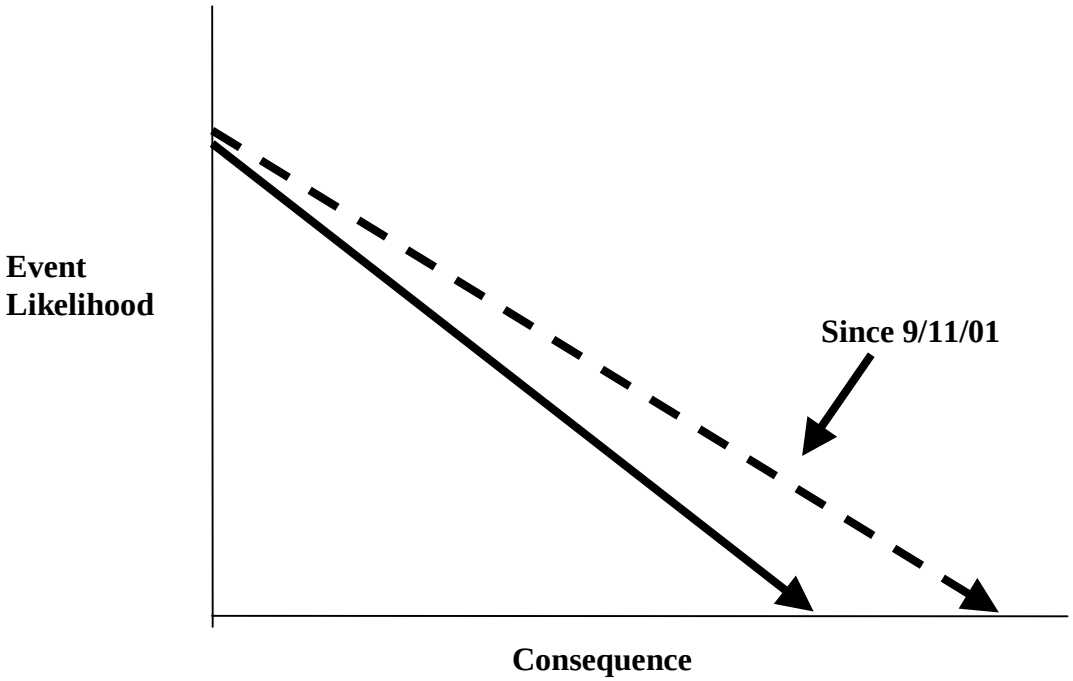

FIGURE 4 Re-visiting incident likelihood.

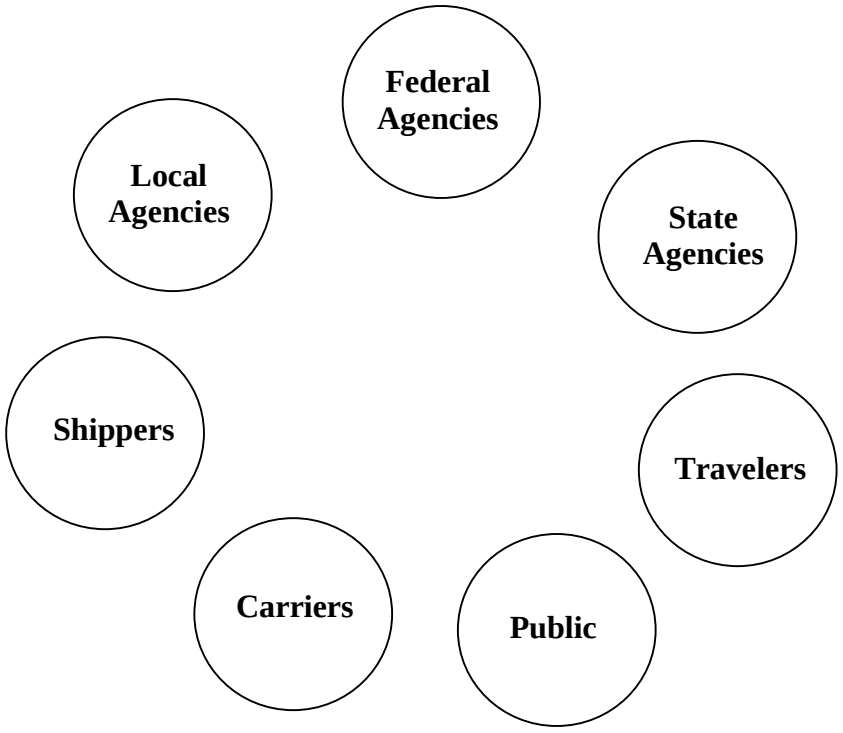

FIGURE 5 The population of transportation risk managers.

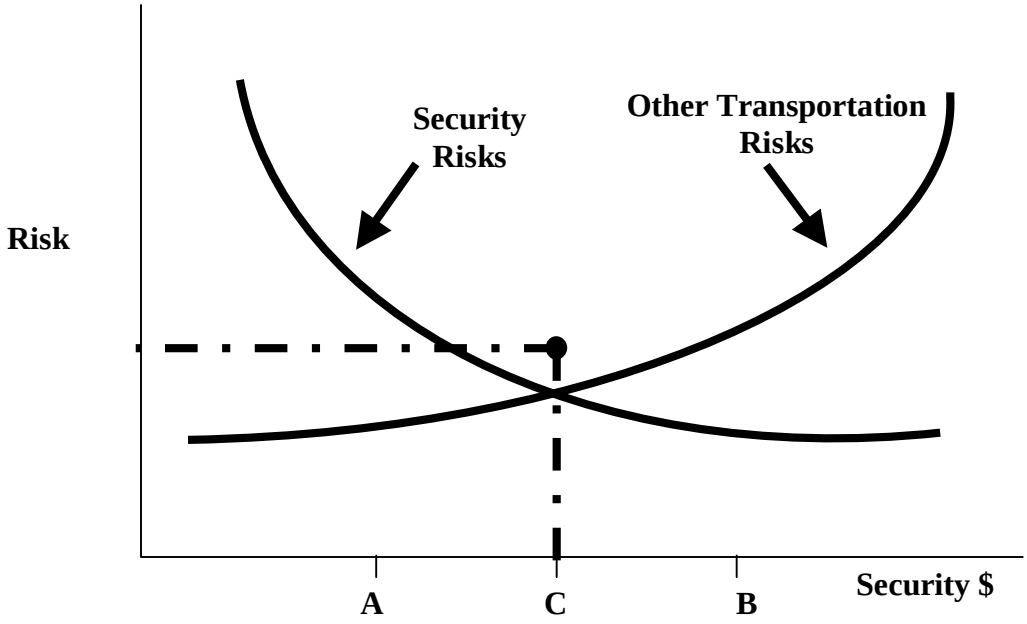

FIGURE 6 Effect of shifting resources from traditional risk management to security initiatives.