Backgrounder

Published by The Heritage Foundation

No. 1889
October 25, 2005

Risk Assessment and Risk Management: Necessary Tools for Homeland Security

Paul Rosenzweig and Alane Kochems

Regardless of their political beliefs, Americans want to prevent another terrorist attack from occurring in the United States. In the face of increasingly diffuse threats and adversaries asymmetrically pursuing vulnerable targets, the question is how can we best prevent such attacks.

Clearly, the United States does not have the extraordinary resources to protect everything, all the time. Therefore, we must allocate our materiel and funding to protect the most critical assets, whether infrastructure or personnel. To assist in prioritizing threats, we must first assess the risks we face and then manage those risks by putting our resources to work in the most effective manner.[1]

Indeed, Michael Chertoff, the Secretary for Homeland Security, made exactly this point earlier this year in announcing the principles upon which the reorganization of the Department would be based. He noted that our "resources are not unlimited" and that tough choices must be made in how they are allocated, using "objective measures of risk."

Those objective measures, he continued, would be based on three variables: threat; vulnerability, and consequences. Most significantly, Secretary Chertoff set forth how he would prioritize the Department's focus, opting to concentrate first on threats "that pose catastrophic consequences" even if these targets are somewhat less vulnerable than other, but less consequential, infrastructure.[2]

Talking Points

- To assist in prioritizing threats, we must first assess the risks we face and then manage those risks by putting our resources to work in the most effective manner.
- Risk assessment takes place in three stages. First is an assessment of near-term threats and an adversary's capabilities. There follows a look at vulnerabilities and how they can be mitigated. Finally, to assist in prioritization, there is a process designed to identify the criticality of various assets—the asset's function or mission and how significant it is.
- The methodology acknowledges an important point too often disregarded by politicians: Risk can only be minimized, not eliminated.
- The federal government is responsible for preventing terrorist attacks through intelligence gathering, early warning, and domestic counterterrorism. The private sector must take reasonable precautions based on its vulnerabilities to limit the ability for terrorists to exploit its weaknesses.

This paper, in its entirety, can be found at:
www.heritage.org/research/homelanddefense/bg1889.cfm

Produced by the Center for Legal and Judicial Studies

Published by The Heritage Foundation
214 Massachusetts Avenue, NE
Washington, DC 20002–4999
(202) 546-4400 • heritage.org

This sort of analysis may sound academic, but it has real world effects. It leads, for example, to the conclusion that we should focus preventive resources on areas of greater concern, like chemical, biological, or nuclear attack. And it leads as well to the conclusion that the Department of Homeland Security cannot and should not be expected to protect Americans from all possible risks. The recent London bombings illustrate the point. A risk assessment analysis asks what the likely consequences of a similar bombing in New York are, and then asks whether or not any reasonable expenditure of resources can prevent those consequences. The likelihood that resources are better spent elsewhere has generated controversy. But as this paper demonstrates, the methodology that the Department proposes to adopt is the right one for America, and should not be discarded because it establishes politically uncomfortable truths.

What Is Risk Management?

Risk is uncertainty. It is both the uncertainty that surrounds actual events and outcomes and the uncertainty that surrounds future, potential events. It may, of course, apply to natural events (like the risk from hurricanes) and to non-physical events (like the risk from changes in the financial markets). As relevant to Homeland Security issues, however, risk is more particularly the likelihood that a terrorist threat will endanger or affect some asset. That asset can be an individual (like the President), a structure (like the Pentagon), or even a function (like America's stock exchange system).[3]

When one thinks of such risks, one must therefore think of any number of underlying elements that go into an evaluation. These might include:

- What is the risk (or threat)?
- What are you trying to protect?
- What is the criticality?
- What/who are the potential actors?
- What are their intentions?
- What are their relevant capabilities?
- Where and what are the relevant weaknesses?
- What are our options to eliminate or mitigate those weaknesses?

As is evident, the assessment of risk depends on many multivariate, contextual factors. To lend structure to the assessment, there is the discipline of risk management.

Risk management is "a systematic, analytical process to consider the likelihood that a threat will harm an asset or individuals and to identify actions that reduce the risk and mitigate the consequences of an attack or event."[4] The methodology acknowledges an important point too often disregarded by politicians: *Risk can only be minimized, not eliminated*.

To lend rigor to the analysis, we try to quantify the risks we experience. Thus, risk may be defined mathematically as probability of the attack occurring multiplied by the probability of success of the attack (or, looked at another way, the inverse probability of failure, interruption, or neutralization) multiplied again by the consequences of the attack

1. This paper is based, in part, on a roundtable held at The Heritage Foundation on February 22, 2005, cosponsored with the Center for Democracy and Technology and the Harvard Belfer Center for Science and International Affairs. The roundtable was an off-the-record discussion and the views contained herein are our own.
2. Michael Chertoff, Second Stage Review Remarks, July 13, 2005, at *www.dhs.gov/dhspublic/display?theme=42&content=4596* (October 20, 2005).
3. Though the threats often differ, the response to occurrences of a threat are often very similar. Our response to Hurricane Katrina is similar in nature to what our response might be to a hypothetical destruction of a large dam by terrorists. That fundamental similarity explains why the Federal Emergency Management Agency should remain a part of the Department of Homeland Security.
4. Raymond J. Decker, "Homeland Security: A Risk Management Approach Can Guide Preparedness Efforts," testimony before the Senate Committee on Government Affairs, October 31, 2001, p. 7, at *www.gao.gov/new.items/d02208t.pdf* (March 15, 2005).

(on some arbitrary relative scale). In mathematical terms that is:

R= Pa x Ps x C

where R is risk; Pa is the probability an attack will be attempted; Ps is the probability of success (or, alternatively 1-Pf, where Pf is the probability of failure); and C is the consequence of the attack).

Threat Assessment

The probability of an attack includes several separate components. It involves, first, an assessment of near-term threats (based, in part, on things like current intelligence and an analysis of the adversary's intentions). In other words, we ask, based upon what we know, what is the likelihood of activity against a particular individual, asset, location, or function.

We then conduct an evaluation of the adversary's capabilities. What can he accomplish with what degree of lethality or effect? Perhaps the biggest change that resulted from September 11 is that we have to fundamentally reassess our adversary's capabilities. When the Soviet Union was the adversary, the capabilities were measured by army divisions and nuclear warheads. Now, they are measured by box cutters. This portion of the assessment is often called the "Threat Assessment."

Vulnerability Assessment

The probability of success (or failure) looks at the other half of the question: What are our vulnerabilities and how can they be mitigated? It involves identifying weaknesses in structures (sometimes physical; more frequently today, cyber structures), other systems, or processes that could be exploited by a terrorist. It then asks what options there are to reduce the vulnerabilities identified or, if feasible, eliminate them.

Criticality Assessment

The consequences factor is intended to evaluate the effect that will be achieved if the adversary accomplishes his goals. Often the goals will include killing individuals, but they may also include social and economic disruption and psychological effects. Not all consequences can be prevented. So in order to assist in prioritization, there is a process designed to identify the criticality of various assets: What is the asset's function or mission and how significant is it?

Nuclear Explosion and Mass Transit Bombings: Two Cases

To take this discussion out of the theoretical and into the practical, consider two distinct possible means of terrorist attack: a nuclear suitcase bomb in New York City and a coordinated series of explosive bombs on the New York subway.

These two examples illustrate, first, the poles of the criticality/consequences assessment. The subway bombing has what risk managers call "thinkable" consequences; the consequences of the nuclear explosion are "unthinkable" ones. The two may be qualitatively distinguished:

- Thinkable risks have few secondary effects and are geographically and temporally bound. However bad an explosion in the subway, its consequences are complete within hours and confined to a small area. For such risks, the goal is to minimize the single points of failure, cascading effects, and uncertainty by focusing on rapid reconstitution and recovery and building security awareness. In other words, we ask people to watch for unattended bags and we provide first responders to limit the aftereffects. Then we act rapidly to rebuild.
- Unthinkable risks, by contrast, involve very large loss of life, great damage, and effects that spread over time and space. For unthinkable risks, prevention is the key. The entities involved need to focus on countermeasures. As a secondary factor they need to look at recovery and, where possible, attribution of blame.

Efforts must be apportioned between thinkable and unthinkable scenarios. For while the probability of a nuclear explosion is low, the impact is so horrific that we must do everything in our power to stop it. By contrast, one can make efforts to stop mass transit bombings, but the principal goal should be to advance speedy recovery. In an aphorism: Thinkable situations need to be made less terrifying while unthinkable ones are made less likely.

Put another way, the virtue of risk assessment methodology is that it frees organizations from

having to rely solely on worst-case scenarios to guide their planning and resource allocation. "Worst-case scenarios tend to focus on vulnerabilities, which are virtually unlimited, and would require extraordinary resources to address. Therefore, in the absence of detailed threat data, it is essential that a careful balance exist using all three elements in preparing and protecting against threats."[5] By contrast, vulnerability assessments identify exploitable weaknesses and suggest ways to eliminate or minimize them and criticality assessments are "designed to systematically identify and evaluate an organization's assets based on the importance of its mission or function, the group of people at risk, or the significance of a structure."[6] Only when an organization makes all three assessments can it assemble a bird's eye view of the situation. Mangers can then use this perspective to create a risk reduction strategy, which guides resource allocation.

Making Risk Management a Reality

Who uses risk management tools and to what end are the important questions. Before risk management can be discussed intelligently, the problems surrounding information sharing need to be resolved. Until the right people are getting the right information in the right format and at the right time, risk management tools will be inefficient and ineffective. Somewhat related to information sharing is the need to form public-private partnerships. Since so many potential terrorist targets are in private hands, the federal government and industry need to divide the protection responsibilities.

Information Sharing

Any risk management system needs to be able to analyze several interdependencies. We live in a complex world with many variables. To understand these variables, there must be trust between data owners and those who want to analyze information to enable sharing. To have effective assessments, one must collect and evaluate as much of the relevant, knowable data as possible.

Yet substantial barriers to information sharing now exist. With 85 percent of critical infrastructure in private hands and numerous other public and private potential targets, risk management faces a substantial information sharing challenge. Private entities have no real incentive to participate in a national risk assessment system. Often the disclosure of information will come with significant costs for the private sector entity—civil liability, competitor enhancement, and the like. At the same time, the central policy issue surrounding risk management is that of resource allocation: Risk assessment can help to determine which threats are important but decision-makers have to decide where to put funding and resources. Not all threats and vulnerabilities can be mitigated or eliminated. Thus, private sector information providers are often left without any concrete benefit. Their vulnerabilities are assessed as lower level risks and having incurred all of the costs, they get none of the anticipated benefits.

To put it prosaically, as one industry representative did (off the record) at a recent conference: "What do we get? If I advise the government of a change in circumstances that present a heightened risk, will I get more police protection? Additional drive-bys? If not, what's in it for me?"

Information sharing is also dependent upon the correct liability framework. Risk management deals in possibilities and probabilities. An analysis tool is only as good as the inputted information. But the potential for liability discourages users from sharing information or doing analysis for fear that, despite their best efforts, they will not be able to stop a terrorist act. Liability caps encourage the use of tools that can improve decision-making while not punishing managers who use such tools if a terrorist attack still occurs.

Defining the Private Sector's Role

It is not the job of the private sector to defeat terrorists. It is the responsibility of the federal government to prevent terrorist acts through intelligence gathering, early warning, and domes-

5. *Ibid.*, p. 3.
6. *Ibid.,* p. 1.

tic counterterrorism. However, it is the private sector's duty to take reasonable precautions, in much the same way as society expects it to take reasonable safety and environmental measures. The federal government has a role in defining what is "reasonable," as a performance-based metric and in facilitating information sharing that enables the private sector to perform due diligence (i.e., protection, mitigation, and recovery) in an efficient, fair, and effective manner. We might consider, for example, whether compliance with a federally developed standard ought to be a bar to all private sector liability.

Thus, a model public-private regime would: (1) define what is reasonable through clear performance measures, (2) create transparency and the means to measure performance, (3) establish ways for the market to reward good behavior, (4) provide legal protections to encourage information sharing, (5) provide some enhanced governmental benefit as an inducement to participation, and (6) ensure that any "fix" does not cripple the economic engine that produces the society and liberties Americans enjoy. Using risk management methods may be one of the reasonable activities in which companies can engage.

Public Education

Finally, since risk management is a widely used tool, education is critical. People need better training on the types of methodologies available and on how to use the technology. They must know the abilities and limitations of their tools—including that risk management cannot tell anyone how to prioritize protection. And even more than the users, there is the need for public education. Everyone involved needs to realize that there is no perfect system and that any reasonable attempt to allocate resources should improve the probability of preventing an attack.

In short, we need to advance to a culture in which we acknowledge the realities of risk. Instead of reacting to the obvious difficulty in defending a mass transit system by yelling at the messenger and throwing more money at the problem, our political system needs to accept that all risks are not avoidable and that sometimes the costs are not worth the benefits.

Conclusion

The federal government is responsible for preventing terrorist attacks through intelligence gathering, early warning, and domestic counterterrorism. The private sector must take reasonable precautions based on its vulnerabilities to limit the ability for terrorists to exploit its weaknesses. The federal government needs to clearly define what are reasonable actions for the private sector and address liability issues. Risk management is one tool for determining where risks and vulnerabilities are. It cannot tell someone, however, how to prioritize targets. It just provides an analysis of strengths and weaknesses so a person can make a more informed decision.

The major impediment to risk management is currently the inability to share information among state and federal governments and the private sector. The government and private sector should work together to form partnerships and to improve the flow of information. To make risk management processes truly effective, people need to be educated on their advantages and disadvantages so that they can use such tools appropriately to help them prioritize and allocate resources.

—Paul Rosenzweig is Senior Legal Research Fellow in the Center for Legal and Judicial Studies at The Heritage Foundation. Alane Kochems is a National Security Policy Analyst in the Kathryn and Shelby Cullom Davis Institute for International Studies at The Heritage Foundation.