Improving Strategic Risk Management at the Department of Homeland Security

By David H. Schanzer and Joe Eyerman

The next contribution is based on a Center report by David H. Schanzer and Joe Eyerman, Improving Strategic Risk Management at the Department of Homeland Security. It explores how the federal government can enhance its capability to use strategic risk management in safeguarding the nation. It focuses on strategic risk management—the process by which decisions are informed by an analysis of risk. Risk management can be applied at several levels: tactical, operational, and strategic. Authors Schanzer and Eyerman describe the recent history of strategic risk management in the department and set forth a series of findings and recommendations directed to the Executive Office of the President, the Department of Homeland Security, and Congress. A key recommendation is that the department should enhance its analytical capability necessary for strategic risk management. The recent creation of an Office of Risk Management and Analysis is an important step toward the department's strengthening its strategic risk management capability and enhancing it decision making process.

America awoke on September 12, 2001, to a world in which our vulnerabilities to previously unimaginable acts of violence now seemed limitless. Al Qaeda had laid bare that our massive infrastructures, our globalized, interconnected economy, and the openness of our society could easily be exploited to cause massive harm to persons, property, and our national psyche. In the weeks and months following the attacks, it seemed that only the limits of one's imagination could confine the number of scenarios in which terrorists could inflict death and destruction on the United States.

One of the strategic responses to the realization of our widespread national vulnerability was the creation of the Department of Homeland Security (DHS), an amalgamation of different agencies and programs from across the government charged with protecting the nation against attacks, reducing our vulnerabilities, and improving our ability to respond to the full range of threats we might face.

Deciding how much of our societal resources to dedicate to homeland security and how to allocate those resources across the myriad of homeland security domains is an exceptionally difficult public policy problem. DHS's efforts to answer these questions through a process called "strategic risk management" is the subject of this article.

Strategic risk management is a highly complex exercise, fraught with difficulties. While significant progress has been made at DHS, theoretical, structural, and political obstacles currently frustrate its ability to allocate its resources based on risk management principles:

- Analytic tools have not been fully developed to deal with the risks created by adaptive adversaries or to compare risks across different threat areas.
- Even if such tools were fully developed, DHS does not have methods for examining the effectiveness of their programs in reducing risk.
- DHS has not developed a core strategic risk management capability as an agency to set priorities and drive budgeting to those priorities.
- Risk tradeoffs are often political decisions that require public input, but mature methodologies for receiving such input have not been developed.
- Congressional legislation mandating various security policies and programs, much of which is not based on strategic risk management principles, diverts DHS from its risk reduction mission.

It is appropriate to evaluate whether DHS is meeting the need to incorporate risk management principles into its resource allocation decisions.

This article seeks to bolster the Obama administration's efforts by first explaining the difficulty of transferring well-established risk management principles and methodologies to the new, still developing field of homeland security. The article then summarizes DHS's current approach toward risk based resource allocation, based on numerous interviews with agency personnel and congressional staff, and identifies

David H. Schanzer is an Associate Professor of the Practice at the Sanford School of Public Policy at Duke University and co-director of the Institute for Homeland Security Solutions, a research consortium between Duke, UNC Chapel Hill, and RTI International, focusing on applied social science research in support of the national homeland security mission. He also is an Adjunct Professor of Public Policy at the University of North Carolina. He teaches and writes about counterterrorism strategy, counterterrorism law and policy, and homeland security.

the hurdles the agency and Congress face in attempting to develop budgets informed by the concept of risk. The final section contains recommendations for the Obama administration and Congress on steps that they can take to enhance government's ability to allocate efficiently the resources available for homeland security to fulfill the constitutional duty to "provide for the common defense."

The Challenge of Applying Strategic Risk Management To Homeland Security

The concept of strategic risk management is not new. Businesses are constantly assessing the risks they face and taking steps to adjust to changing circumstances—whether by selling or purchasing new assets, taking on or reducing debt, or increasing or reducing their workforce. On a micro level, families are risk managers as well. We are constantly assessing risks that we face and responding. We purchase insurance to shift certain risks to others. We take steps like fixing an old roof or getting more exercise to mitigate risks to our property or personal health. Certain risk we choose to accept—like the risk of driving to work or allowing an old tall tree to remain right next to our home. The range of choices we make in our lives is, in a sense, a form of strategic risk management.

Application of strategic risk management to the concept of homeland security, however, is a relatively new and poorly understood topic. This section discusses the need to apply strategic risk management to homeland security and identifies many of the difficult challenges of incorporating concepts and tools developed in other areas to this new and evolving area.

Increased funding for enhanced homeland security flowed freely in the initial months following 9/11 through supplemental appropriations measures and large increases for particular programs, such as transportation security. Creation of the DHS brought greater focus to the question of homeland security funding that became the topic of political discourse between Congress and the executive branch, as well as a dialogue between the federal, state, and local branches of government.

While there is no agreed-upon definition for the term "risk," in its new publication, *DHS Risk Lexicon,* the department's extended definition of risk is "potential for an adverse outcome assessed as a function of threats, vulnerabilities, and consequences associated with an incident, event, or occurrence."

By developing tools to make mathematical calculations of these factors, risk science can provide a means of assessing the risk reduction value of a given policy, program, or budgetary investment. Even in fields where risk science is well developed, such as environmental protection, results of risk analysis are still only tools that inform decision making and cannot dictate policy results or replace the need for judgment.

Identifying risk management as a core principle guiding DHS activities made a great deal of sense. Yet, putting this concept into practice in the homeland security domain has proven to be a daunting task. From the earliest days after creation of the department, many placed faith in the idea that we could develop a formula or matrix that could answer the questions such as, "How much should we be spending to keep us safe?" or "Should we be spending more money on chemical detectors on subways or new anthrax vaccine?"

The calls for improved risk management have not only emanated from Congress. The 9/11 Commission was among the first of many expert panels to raise the topic, concluding that homeland security funds should be allocated "based on

Joe Eyerman is the co-director of the Institute for Homeland Security Solutions (IHSS) and the director of RTI's Health Security Program. Dr. Eyerman has more than 17 years of professional experience statistically modeling social behavior and managing data for the analysis of political behavior and conflict. His substantive interest is in the modeling of decision processes related to political behavior, group decision making, multi-agency coordination, and political conflict. His recent methodological work has focused on the relationship between the data collection process and error in population estimates on a variety of bioterrorism, public health, and surveillance studies.

an assessment of threats and vulnerabilities." In 2007, the Government Accountability Office convened an expert panel to identify and address risk management challenges.

In 2008, on the seventh anniversary of 9/11, the Homeland Security Advisory Council listed improving risk management among the top challenges for DHS. The Council concluded:

> Determining the risks to Homeland and using a risk management approach to allocate resources, make decisions, and communicate threats, readiness and protective actions has not been perfected. This will require establishing and improving performance metrics for measuring risk and building a framework for risk-informed decision-making.

While the need to apply strategic risk management principles to homeland security is well-founded and compelling, it is important to understand the difficulties of applying this well-established methodology to the new and evolving discipline of homeland security.

One can begin to grasp the enormity of the task of developing a unified, comprehensive risk assessment that can be used to guide DHS's budget allocation decisions. All the factors that comprise threats are enormously difficult to calculate. Threats (not only from terrorism, but natural disasters and unintentional accidents) are extensive, varied, and uncertain. The scale of estimating the vulnerabilities in our complex, diversified, and densely populated country are massive. And calculating the consequences of a possible event is complicated by the interconnected nature of our economy, where small impacts in one area could have spiraling ripple effects throughout the economy.

Furthermore, we have been using risk science to attempt to inform decision making in areas like environmental protection and workplace safety for decades, but are just beginning to develop methods for quantifying the elements of risk with respect to homeland security. We have well-established models to predict how changes in policy will affect the level of air pollution on the population, but these models just don't exist for predicting terrorist attacks.

There is a great degree of uncertainty as to when, where, and how terrorists will attack. Moreover, terrorists are adaptive adversaries. Any action we take to prevent a particular type of attack will lead to a change in the terrorists' strategy and tactics that may render the protective action moot. Take, for example, chemical plant security. Intelligence might suggest that terrorist organizations intend to infiltrate a plant and detonate an explosive. In response, we invest millions installing surveillance cameras and otherwise improving perimeter security. Yet, having observed our build-up in perimeter security, the terrorists merely switch tactics to highjacking a rail chemical container in transport.

Measuring risk is also uncertain because we do not know how populations and governments will respond when attacks occur:

- Will there be mass panic, causing huge consequences, or will a response be orderly and effective?
- Will governments respond in a manner proportionate to the risk, or will they overreact and inflict unnecessary harm on economy or the social fabric of society?

We also have to take into account that not only are these risks objectively uncertain, but individuals will have varying subjective evaluations of risk levels (which helps explain why some people evacuate when a hurricane is approaching and others go surfing).

Finally, homeland security problems often involve multiple stakeholders who have varied interests. Take, for example, the issue of screening cargo in foreign ports—which seems to be a commonsense security measure. Any decision regarding these foreign inspections, however, implicates diplomatic relations with the other countries, multiple corporate stakeholders, unknown and unpredictable impacts on the global supply chain, government employment issues, protection of proprietary information, data integrity issues, and customs collection matters to name but a few of the stakeholders and interests.

Strategic Risk Management Is a Process, Not a Formula

All of these difficulties make analyzing homeland-security risks an especially "wicked" problem. Such problems are not amenable to solutions based on simple risk formulas, but rather require discourse based, multiparty conflict resolution techniques. In an ideal world, DHS would be able to produce a list of our top five security priorities with a scientific formula explaining how the ranking was developed and how federal spending will systematically reduce the societal risk our nation faces. But this notion is entirely unrealistic.

Not only is it important to understand that risk management is a process of governance, but also that risk management is a continuous cycle. The Government Accountability Office has developed a risk management cycle representing the ongoing nature of this process. As Figure 1 indicates, the first step is developing strategic goals based on inputs from the intelligence community concerning threats, the existing legal and policy framework, the availability of technology to address the identified risks, and public input. This is followed by a process of assessment, whereby the causes of the risks are identified, possible means for mitigating risk are evaluated, and the cost and benefits of the courses of action are calculated. Policymakers must then select a course of action, which entails assigning responsibilities and providing resources. The policy is then implemented and, importantly, evaluated. These evaluations then inform the revision of the strategic goals, and the process begins anew.

Figure 1: GAO Risk Management Cycle

Risk Management at the Tactical, Operational, and Strategic Levels

Risk management activities are needed and are taking place at DHS at several levels:

- **Tactical risk management** refers to the process for selecting among alternative courses of action that are permitted within a given policy. An example of tactical risk management at DHS is the Coast Guard's process for determining the place of refuge for a distressed vehicle when it needs to enter a port for repairs.
- **Operational level decisions** require selection among policy options to achieve a stated objective. For example, the Transportation Security Administration is using risk management techniques to select among the various options for providing enhanced aviation security.
- **Strategic risk management** is the process through which these decisions are informed by the concept of risk. This paper is focusing on decision making at the strategic level—where the entire agency establishes goals, sets policy to meet those goals, and then allocates resources to implement policy.

Risk Management Through Strategic Planning

Developing a risk management approach requires the infusion of risk management principles at all levels of DHS's planning process. The strategic plan ultimately drives the budget process and the allocation of resources to specific programs.

DHS's Strategic Plan for fiscal years 2008–2013 establishes five goals for the agency:

- Protecting the nation from dangerous people
- Protecting the nation from dangerous goods
- Protecting critical infrastructure
- Strengthening preparedness and emergency response capabilities
- Strengthening and unifying DHS operations and management

Strategic Risk Management Through Budgeting

Only recently have efforts been made to apply risk management techniques to the DHS budgeting process. DHS's early budgets were, in essence, a combination of budgets from its legacy components plus budgets from new components designed to start programs and build capabilities as quickly as possible. There is no evidence that efforts were made in the early days of DHS to systematically assess risks and

A Simple Example of Strategic Risk Management in Homeland Security

The difficulty of developing methodologies to manage the full range of security risks for which DHS is responsible is best explained through a simplified example: How should DHS decide whether to spend an available $5 million on security improvements to the Lincoln Tunnel in New York or on bio-protection suits for first responders in Los Angeles?

Improvements on the Lincoln Tunnel would be important because:

- Terrorists have struck in New York before and therefore are likely to do so again
- The tunnel has vulnerabilities that could be exploited by a terrorist attack to damage it
- If the tunnel is damaged, a large number of people could be killed and there would be severe economic consequences to the local and regional economies

Spending on bio-protection suits in Los Angeles could also be justified because we know that:

- Terrorists have expressed interest in bioterrorism and we believe they are capable of executing a bioterrorist attack
- Biological pathogens can be manufactured and spread throughout large population centers to make people ill
- If there is a bioterrorist attack, having trained and well equipped emergency first responders could save lives

Strategic risk management is a discipline that provides tools that begin to help us make these types of decisions. The concept of "risk" is helpful because it ties together the variables reflected in the example above by defining "risk" as the function of threat, vulnerability, and consequence (R = T x V x C). In this formula, threat equals the likelihood that an attack could occur (which has two components—what the terrorists' intentions are, and their capability to execute such an attack). Vulnerability reflects the likelihood that an attack, if launched, would be successful. Consequences are the total impact that an attack would cause, including both tangible (deaths, damage to property, economic losses) and non-tangible impacts (such as effects on consumer confidence or national pride).

Applying these concepts to the example above, we could attempt (in this grossly simplistic way) to apply risk scores to the two attack scenarios. On a scale of 1 to 10, we might apply a 7 to the threat of a bomb attack on the Lincoln Tunnel, we could say that the bomb terrorists are capable of delivering to that target has a 50 percent likelihood of breaching the tunnel wall, and then estimate that the total consequences of such an attack in terms of lives lost, property and economic damage, and psychological tolls are $2.0 billion. This would give the bomb scenario a risk score of 7 billion. Whereas we could score the threat level of the bioterror attack in Los Angeles as a 5, the likelihood that such an attack would infect 100,000 people at 25 percent, and estimate the consequences of such an attack would be 1,000 deaths and 25,000 long-term illnesses at a cost of $5 billion, for a total risk score of 6.25 billion.

To answer our question about the relative value of the two proposed expenditures, we would need to estimate how each intervention would impact the overall risk. If the hardening of the tunnel wall would reduce the vulnerability from 50 percent to 25 percent, that would lower the tunnel risk score to 3.5 billion. If buying protective suits for first responders would reduce the consequences from $5 billion to $1 billion—that would reduce the risk score of the bioterror attack to 1.25 billion. Under this crude analysis, we lower the overall risk to the nation more with the expenditure on bioterror suits than hardening the Lincoln Tunnel. The concept of risk gives us at least some way to inform comparative judgments across dissimilar domains.

allocate funds according to a strategic plan to reduce these risks as cost effectively as possible. Of course, this is understandable in light of the way DHS came into being—moving from a presidential proposal to authorizing legislation to swearing in of the first secretary in about seven months.

As Cindy Williams describes in her paper for the IBM Center for The Business of Government, the annual budgeting process is supposed to begin with a threat assessment presented by the DHS Office of Intelligence and Analysis to identify emerging and declining threats. The planning process culminates in the preparation of the Integrated Planning Guidance, a memo from the secretary to DHS's components that discusses strategic goals, describes policy priorities, and provides fiscal guidance.

Our research confirmed Williams' conclusion that the front end of the planning, program, budgeting, and execution (PPBE) process "remains weak." The comprehensive threat assessment was not included as part of the planning process until the 2008 to guide development of the fiscal year 2010 budget. During that budget cycle, cross-component leadership meetings were held to review these threat assessments and establish departmental-wide priorities. These priorities were communicated to the components whose budgets are supposed to be responsive to the guidance produced during the cross-component meetings. Guidance from these cross-component meetings, however, was considered to be "one input among many."

In addition to these steps, DHS is developing a decision tool to attempt to inform its resource allocation process—known as Risk Assessment Process for Informed Decision-Making (RAPID). This program is being implemented by the Office of Risk Management and Analysis, created in April 2007 to develop a common framework across DHS to analyze and manage homeland security risk. This small office, located within the National Protection and Programs Directorate, was initially formed outside of the normal budget cycle with limited resources.

RAPID has identified 85 risk reduction areas (such as screening cargo for nuclear material) and mapped them against the priority goals identified in the DHS strategic plan. DHS's programs were then surveyed to identify the risk reduction areas that each program addressed. This tool is intended to provide a means to identify gaps in programming and allocate resources to programs when new strategic goals are developed or strategic priorities are shifted. It also provides a framework for program managers to justify their budgets in terms of how they contribute towards DHS risk reduction areas and strategic objectives. Although the program has been in development for over two years, it is not currently delivering quantitative results that can be used to influence the strategic planning or budgeting process.

Strategic Risk Management Through Evaluation

One aspect of the risk management process that is given too little attention is program evaluation. There is often an assumption that the development of a new program, a change in policy, or expenditure of funds will reduce risk in the manner intended. One security function that has been rigorously evaluated is the effectiveness of airport screeners, and we have learned, over time, that increased professionalism, training efforts and technological improvements have not reduced the rate of illicit materials entering security efforts to the degree that policymakers expected or desired.

The vast majority of DHS security programs, however, have had no or virtually no rigorous, independent evaluation to determine effectiveness. One DHS official noted that the agency was "at a prototype stage on the way to a pilot stage" for developing measurements of program effectiveness. The RAPID program, for example, uses subject matter experts to opine on program effectiveness because program evaluations (and even the means to evaluate such programs) are lacking.

The inability of DHS to measure comprehensively the baseline requirements and the effectiveness of its programs is a major hindrance to effective strategic risk management. It is virtually impossible to allocate resources based on reducing potential harms from security risks unless it can be determined that programs in which resources are being invested will actually work.

Impact of Congress on DHS's Strategic Risk Management Efforts

Most discussions about DHS's difficulties developing strategic priorities and mapping resources against those priorities focus on deficiencies at the agency itself. It is important to recognize, however, that Congress plays an integral role in shaping the internal operations of DHS, allocating resources, and establishing legal mandates that DHS must meet, regardless of their risk reduction value. To better align DHS's resource allocations with their risk reduction value, therefore, Congress must be a risk manager as well.

The challenge will be to develop a jurisdictional and oversight regime that reflects the multi-disciplinary nature of DHS, while controlling the oversight burden and protecting the agency from overbearing congressional activities that divert the agency from its core priorities.

Findings and Recommendations

To the Executive Office of the President

Finding One: The concept of homeland security has not been clearly defined.

Recommendation One: The president should issue an Executive Order that defines the homeland security mission and allocates responsibilities across agencies.

Finding Two: The federal government lacks a cross-department risk reduction strategy.

Recommendation Two: The president should establish a Cabinet-level working group on domestic risk management to coordinate approaches towards risk.

Finding Three: Efforts to explain risk management principles to the public have been weak.

Recommendation Three: The president should discuss risk priorities with the American people.

To the Department of Homeland Security

Finding Four: The budget process provides few opportunities for cross-agency deliberation on priorities.

Recommendation Four: The secretary should establish a budget process that requires cross-agency deliberation over budget priorities.

Finding Five: The DHS strategic planning process does not sufficiently incorporate risk management principles.

Recommendation Five: The assistant secretary for policy should use risk management principles to inform strategic planning.

Finding Six: DHS lacks core analytic capability to execute risk management.

Recommendation Six: The undersecretary for management, the undersecretary for science and technology, and the assistant secretary for policy should propose budgets that build DHS's analytic capabilities for risk management. In addition, the department should clarify the roles and responsibilities between the DHS units that undertake strategic risk management.

Finding Seven: DHS does not systematically evaluate its programs.

Recommendation Seven: The undersecretary for management should require that program evaluations be incorporated into all major program budgets.

To the Congress

Finding Eight: Congress has enacted legislation imposing mandates on DHS without evidence that they reduce risk.

Recommendation Eight: Congress should enact legislation requiring risk management impact statements to accompany all homeland security legislation.

Finding Nine: Congress is frustrated that DHS has not articulated a risk-informed set of priorities.

Recommendation Nine: The chairmen of the Senate and House Appropriations Committees should convene an annual risk management summit between DHS and key congressional homeland security leaders.

Finding Ten: Duplicative and excessive oversight from congressional committees presents difficulties for DHS.

Recommendation Ten: The Speaker of the House and Senate Majority Leader should coordinate congressional oversight of DHS. ■

TO LEARN MORE

Strategic Risk Management in Government: A Look at Homeland Security
by David H. Schanzer and Joe Eyerman

The report can be obtained:

- **In .pdf (Acrobat) format at the Center website, www.businessofgovernment.org**
- **By e-mailing the Center at businessofgovernment@us.ibm.com**
- **By calling the Center at (202) 515-4504**