Risk Management and the Office of Homeland Security's Antiterrorism Tasks

Bin Jiang

Introduction

The Project Management Institute (PMBOK, 1996) defines a project as "A temporary endeavor undertaken to create a unique product or service." It is specific, timely, usually multidisciplinary, and always conflict ridden.

After the September 11 tragedy, President Bush established The Office of Homeland Security. Even though the Office has a routine mission – to develop and coordinate the implementation of a comprehensive national strategy to secure the United States from terrorist threats or attacks – it will fulfill this mission by many individual endeavors to detect, prepare for, prevent, protect against, respond to, and recover from terrorist attacks within the United States. Each such endeavor is a unique and temporary project, focusing on special suspects or targets and terminating when potential dangers are eliminated.

A project will have many other distinguishable characteristics including uncertainties as well as being unique and temporary. Projects are unpracticed, unrehearsed, and are prone to internal and external uncertainties and risks. To successfully carry through each task (project) and to provide the unique product (national security), The Office of Homeland Security must deal with the risk – terrorist threats or attacks.

The statement, "If they (terrorists) want to get you, they will," is often made, seldom challenged, and false. The active combatant (terrorist) always maintains an advantage over the reactive combatant (U.S.) (Rancich, 2000). To thoroughly win the antiterrorism war, The Office of Homeland Security should apply modern risk management theories to its antiterrorism endeavors.

Lock (1997) acknowledges the concept of risk in his definition of project management. He outlines: "The purpose of risk management is to foresee or predict as many of the dangers and problems as possible and to plan, organize and control activities so that the project is completed as successfully as possible in spite of all the risks."

Risk Identification

Project risk management includes the processes concerned with identifying, analyzing, and responding to project risk (PMBOK, 1996).

What is risk?

Burke (1999) defined risk as "a potential future problem that has not yet occurred that prevents or limits the achievement of your objectives as defined at the outset of the project." Risks may be internal, those within the control of the organization such as security services in the World Trade Center or external those risks that are uncontrollable by the organization such as terrorists' attack plans.

Risk identification consists of a thorough study of all sources of risk in the project (Mantel, Meredith, Shafer and Sutton, 2001). Common sources of risk include the organization of the project itself; senior management of the project organization; the client; the skills and character of the project team members; acts of nature; and so on.

A terrorist attack is not asymmetrical. The terrorist has a mission essential task list that he must fulfill to conduct operations. He has to recruit, train, and deploy – all points at which he can be detected (Rancich, 2000). We can estimate the attributes of the force – small, covert, highly trained, and committed. The attack likely will be close in and rapid. The weapon most likely will be a vehicle bomb or small arms, with a good probability of future chemical or biological capability.

To identify risks, Lanza (2000) categorized risks as follows:

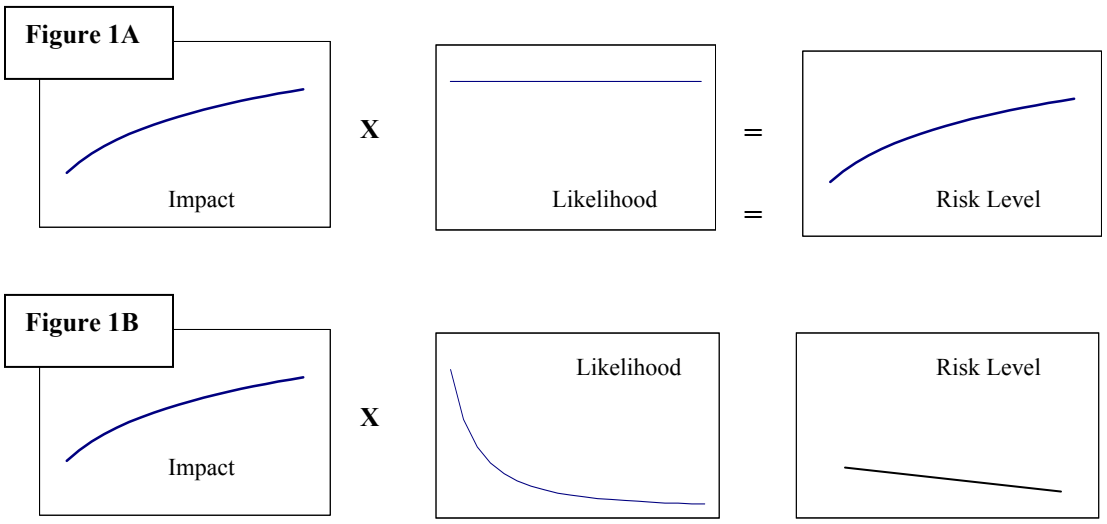
- Known risks – risks whose existence and effects are known (e.g., terrorists use hijacked commercial airplanes to crash into the national icons);
- Unknown known – risks whose existence is known but whose effect is not (e.g. terrorists possess chemical and biological weapons); and
- Unknown unknowns – risks of which there is no awareness at the present time of their existence and effect (e.g., during and after Afghanistan war, the strategy and capacity of Islamic terrorists).

The arithmetic of risk

After the major risks are identified, the following data should be obtained on each to facilitate further analysis (Mantel, Meredith, Shafer and Sutton, 2001): the probability of each risk event occurring; the range or distribution of possible outcomes if it does occur; the probabilities of each outcome; and the expected timing of each outcome.

According to Smith (1999), the level of risk is the product of two factors: 1) its impact (e.g., low, medium, high), which is the severity of the risk should it occur, and 2) the likelihood of occurrence (e.g., 30% chance of happening).

In reality, there is little we can do about the risk's impact. For example, the appearance of Anthrax will bring a great fear to the relevant community. However, the key to managing risk is usually to control the likelihood of its occurrence, constantly driving it down as we progress. The risk is still there, but we manage it by reducing the chance that it will hurt us. This is the difference in figures 1A and 1B.



Risk Analysis

Once we have identified our risks, we need a way to prioritize and track them. The essence of risk analysis is to state the various outcomes of a decision as probability distributions and to use these distributions to evaluate the desirability of certain managerial decisions.

There are many risk analysis tools, such as Monte Carlo simulation, game theory approach, Crystal Ball, risk map, and so on. All of them just try to answer three basic questions: What can happen? How likely is it to happen? What are the consequences if it happens? Risk map is the simplest one, but it thoroughly reveals the core of risk analysis: impact and probability decide the priority of risk together.

Smith (1999) put risks in a chart, such as Figure 2. The two axes represent the likelihood of occurrence and the impact. He refers to this process as "mapping risk." To demonstrate the technique, we can map six risks in Figure 2. The illustrative risks are:

- HCP: Hijack Commercial Plane;
- CBA: Chemical-Biological Attack;
- PWS: Poison Water Supply System;
- ALB: Attack Long-Distance Buses;
- FPB: Fire Public Buildings; and
- ANR: Attack Nuclear Reactors.

Once last element appears in Figure 2, the curved line of constant level of risk, which follows from the arithmetic-of-risk discussion. This line forms a threshold; any risk above it is deemed important, so it comes under active risk management. Risks below the threshold line are not actively managed.

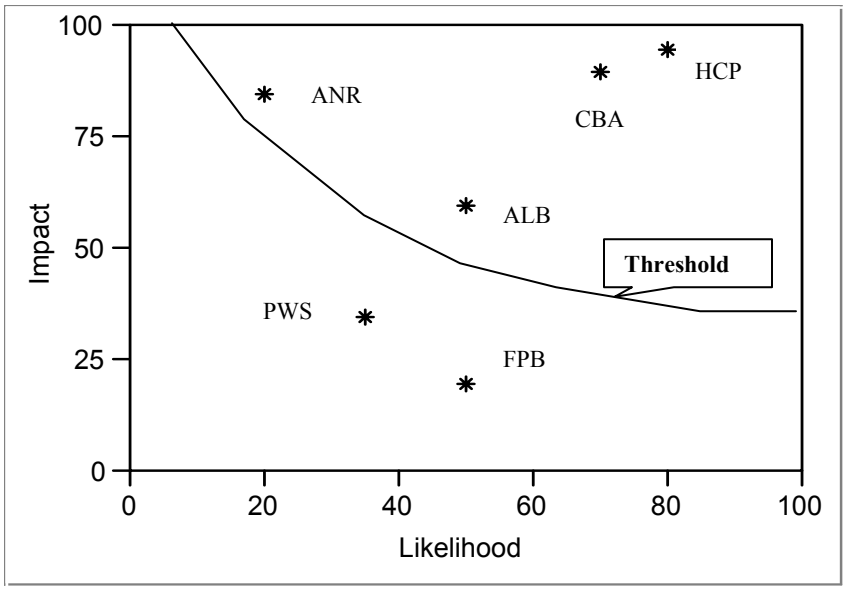


Figure 2

Smith (1999) pointed out: "You set the threshold line according to your tolerance for risk. If you move it lower, you will be bringing more risks under active risk management, thus reducing your overall level of risk. However, you will also be paying more to manage this larger group of risks. In other words, you obtain more protection by buying more insurance." Any risk above the threshold line receives active risk management, which means that we devise an appropriate plan to manage that risk. Managing it usually means driving its likelihood of occurrence down.

Recognize that a terrorist act is a low-probability/high-impact event and build a program that is specific to probability, threat, and political/fiscal restrictions. Rancich (2000) believed that we should establish such an effective program to identify the most likely and highest impact possibilities and then detail actions taken/risks mitigated and actions not taken/risks not mitigated, along with a logical rationale for each.

The fundamental idea of risk assessment is: when we assess risks, the first thing we have to determine is what our vulnerabilities or exposures are. Vulnerability or exposure is a weakness that enables a risk to have an impact. Without vulnerability or exposure, risks will not work. Defining vulnerabilities will allow the Office of Homeland Security to better bring its limited assets to bear.

For example, after the USS Cole was attacked by a small explosive-laden boat in Yemen, the U.S. Navy found that pier access control is a vulnerability. By defining that weakness, the Navy took specific action to prevent it from happening. The Navy is not concerned that sailors are walking on the pier, so it should not waste assets on controlling those actions. By defining its real, operational concerns, the Navy concentrated assets on stopping specific threats, resulting in both better antiterrorism security and economy of force.

Response to Risk

Now that we have a risk map and a group of plans for the risks currently above the threshold line, we should make a decision about which risks to prepare for and which to ignore and simply accept as potential threats. This part is the final output of the entire risk management process. It should be the most exciting, the most breathtaking, and the most innovative movement. Though the Office of Homeland Security will apply totally different responses to each special risk, there are still some general principles of risk response in play.

In general, there are six possible decisions on risk response (Lanza, 2000, Bullen, 2001, and Kliem, 2001). To *prevent* a risk means eliminating the cause before it is an issue. To *accept* a risk means letting it occur and taking no action. To *avoid* a risk is to take action to not confront a risk. To *adopt* a risk means living with a risk and dealing with it by "working around it." To *transfer* a risk means shifting a risk over to someone or something else. To *migrate* a risk means reducing the probability that this risk will occur.

No matter which action plan the Office of Homeland Security takes, the key determinant as to whether to take a more stringent approach (e.g., prevention) is dependent upon the cost/benefit relationship surrounding that risk.

Based on the risk categories, the following list provides a response for each known/unknown risk category (Lanza, 2000):

- Known risks -- If the effect of the risk is large, chart a new strategy to prevent the risk or, if the risk effect is small, mitigate or accept the risk;
- Unknown/known risks -- First, estimate the effect of the risk and, depending on the projected risk magnitude, use the strategies explained for "known risks"; and
- Unknown/unknowns risks -- As much as the likelihood and magnitude of this risk cannot be predicted, it is wise to add a contingency estimate to the project – for example, adding 10% of cost to a financial plan for "contingency allowances" without knowing exactly where this reserve will be applied.

Remember that the risk response is a continuous process, involving ongoing work on each of the plans, as well as keeping the risk map up-to-date. The updating has five components (Smith 1999):

- Replotting the risks under active management (usually they will be moving to the left);
- Replotting the risks below the threshold line (they can move in any direction);
- Identifying any new risks that have arisen and locating them on the map;
- Generating action plans for any risks now appearing above the threshold line; and
- Terminating the action plans of those risks that have moved below the line.

Conclusion

Terrorism is an unconventional operation that the U.S. confronted with conventional security means before. The terrorist is involved in extended operations to achieve his organization's long-term goals, but the U.S. was defending an infinite number of single moments, with short-term achievement as the only defined goal. The U.S. was fighting a strategy with tactics (Rancich, 2000). So the terrorists took the proactive positions, but the U.S. took the reactive positions.

However, terrorism is not magic. We may not know when or where the next attack is going to take place, but that does not prevent us from preparing by actively applying risk management tools. Under the risk management microscope, we can easily find out where our most vulnerable exposures are and which risks have high priority. Then we can select the appropriate risk responses to pursue our national security.

References

J. Bullen, "A Critical Assessment of the Key Elements of Successful Project Management," *Working Paper for the Business Information Technology Department of the Canterbury Christ Church University, Kent, UK.* March 12th, 2001.

R. Burke, *Project Management Planning and Control*, 230 1999, West Sussex, Wiley.

R. Kliem, "Managing and Controlling Risk," *Year 2000 Practitioner*, Jan 1999, Vol. 2 Issue 1, p14.

R. Kliem, "Risk Management for Business Process Reengineering Projects," *Information Systems Management*, 71-73 Fall, 2001.

R. Lanza, "Does Your Project Risk Management System Do the Job?" *Information Strategy: The Executive's Journal*, 6-12 Fall 2000.

D. Lock, *The Essentials of Project Management Gower*, 1-3, 1997.

Mantel, Meredith, Shafer and Sutton, *Project Management in Practice*, 101-105 2001, John Wiley & Sons.

PMBOK (*A Guide to the Project Management Body of Knowledge*), Project Management Institute, 111-121 1996.

T. Rancich, "Combating Terrorism," *U.S. Naval Institute Proceedings*, Nov 2000,Vol. 126 Issue 11, 66-69.

P. Smith, "Managing Risk as Product Development Schedules Shrink," *Research & Technology Management* 25-32 (September-October 1999).

Office of Homeland Security - description of the office and Homeland Security Council headed by Governor Tom Ridge. http://www.whitehouse.gov/news/releases/2001/10/20011008.html

---

Bin Jiang *is a doctoral student in the Collage of Business Administration at University of Texas at Arlington. His primary research interests utilize statistical methodology to create new methods for operations research problems appearing in business and engineering. He has his MBA degree from the Marshall School of Business at University of Southern California.*