ABSTRACT

Virginia’s Critical Infrastructure Protection (CIP) Study implements risk assessment and management methodologies upon eight case studies located in the commonwealth of Virginia. Research was undertaken because of a growing national concern involving infrastructures that are so vital that their incapacity or destruction would jeopardize the security of the United States. Furthermore, the project’s pertinence is palpable in the wake of 9-11. The report demonstrates the efficacy of the risk assessment and risk management methodologies and its output will be utilized in the development of a computer-based tool for use by Virginia Department of Transportation (VDOT) employees. The net result of the project’s analysis extends beyond the immediate benefits of the risk management output generated by individual case studies. Rather, the analysis below helped highlight errors and highlight commonalities that will be utilized in the development of a more robust and more effective computer-based risk management tool.

1 INTRODUCTION

1.1 Background

Since the terrorist attacks of September 11, 2001, the Bush administration has taken tremendous steps to establish the United States as the leader of the free world in the fight against terrorism. In particular, President Bush created the Department of Homeland Security (DHS) to “prevent terrorist attacks within the United States, to reduce America’s vulnerability to terrorism, and to minimize the damage and recover from attacks that may occur” (Bush, 2002). In order to achieve these objectives, the DHS has made protection of the nation’s critical infrastructure a top priority. The nation’s critical infrastructure refers to 13 critical infrastructure sectors including the transportation system (U.S. Dept. of Homeland Security, 2003). Critical infrastructures, as defined by Congress in the USA Patriot Act, are those “systems and assets, whether physical or virtual, so vital to the United States that the incapacity or destruction of such systems and assets would have a debilitating impact on security, national economic security, national public health or safety, or any combination of those matters” (sec. 1016(e)).

While the DHS will coordinate a national effort, state and local governments must also assume the responsibility of securing America’s critical infrastructure. Before the establishment of the DHS, relatively little effort had been made to safeguard the surface transportation infrastructure against terrorism nationwide. Characterized by an unyielding commitment to safety and security, the Virginia Department of Transportation (VDOT) has been and continues to be a forerunner in this imperative effort. VDOT has recognized that the surface transportation system is particularly vulnerable to terrorism due to its size, accessibility, and numerous interdependencies with other critical infrastructures such as emergency services and the government. In addition, Virginia’s transportation system is particularly vital as it contains major east/west connectors for travelers in the mid-Atlantic region and the second most complex system of underwater tunnels and bridges in the world.

1.2 Scope

This study addresses the need to manage the risks of terrorism to the surface transportation system in Virginia. This is achieved through the implementation of a methodology for identifying, prioritizing, and mitigating the risks from potential terrorist attacks to eight critical assets within Virginia. Critical assets of the transportation system, such as major bridges and tunnels, are the most susceptible to terrorist attacks owing to their size, complexity, usage, func-
tions, and location, among other things. The eight critical assets analyzed in this study include:

- One Intelligent Transportation System (ITS) traffic-control center
- Two major interstate interchanges
- Three bridges
- One bridge-tunnel
- One tunnel

Furthermore, this study tests the efficacy of the risk management methodology for use on transportation assets. Problem areas were highlighted and will be acknowledged in the ultimate design of the computer-based risk management tool.

2 RISK ASSESSMENT

The CIP project began with a risk assessment analysis of each of the case study sites. Risk assessment involves answering three questions about a site. According to Kaplan and Garrick (1981) these three questions are:

1. What can go wrong?
2. What is the likelihood that something will go wrong?
3. What are the consequences if something does go wrong?

The general methodology followed for this process was the Risk Filtering, Ranking, and Management (RFRM) methodology developed by Yacov Y. Haimes, Stan K. Kaplan and James H. Lambert (2002).

2.1 Identification of Vulnerabilities

Phase I of RFRM involves a process called Hierarchical Holographic Modeling (HHM) (Haimes 1981, 1998). HHM allows the decision maker to look at all aspects of a system, including the interdependencies between the different aspects. Furthermore, not only can the decision maker identify the sources of risk for a system, he can identify exactly what the causes of each of those sources could be. As noted by Haimes and Longstaff (2002), “A comprehensive holistic modeling schema is needed to do justice to the complexity of critical interdependent infrastructures. In hierarchical holographic modeling (HHM), the analyst can address (and quantify to the extent needed and possible) the essence of their important and relevant characteristics” (262). While HHM can be used to perform a complete risk analysis, it can also be used to perform a partial analysis without losing anything any vital information. In the context of this project, “partial” does not mean an incomplete assessment of the risks posed to the infrastructure assets by terrorists; rather, it means that the case study focused only on the risks posed by terrorism, as opposed to looking at every possible risk. Developing the HHM for the case study sites involved researching the sites and talking with the site managers to get their input on where they thought the sites were vulnerable. Figure 1 shows a sample HHM.

![Sample Hierarchical Holographic Model (HHM)](image)

Figure 1: Sample Hierarchical Holographic Model (HHM)

Phase II of RFRM involves filtering the HHM to eliminate any unnecessary areas of risk. For example, Figure 1 shows a category of risk to an interchange asset called “Geographic Coverage.” At this phase of the risk assessment process, this topic was eliminated because even though the interchange studied in this HHM is actually three separate interchanges, they are all close enough to affect each other. It was therefore decided that they could be considered one system for the sake of simplicity, thus meaning that the “Geographic Coverage” category of the HHM was irrelevant.

Much of this filtering was done automatically in Phase I of this project because the project was already focusing on a particular area of risk to critical infrastructure, namely willful threats and terrorism. This was taken into account as the HHM for each case study were developed, so there were only a few areas of risk that needed to be filtered out in this phase. This particular phase would be more applicable in a situation where a full HHM had been developed, and later it was decided that the study was to focus on a particular area.

2.2 Threat Scenarios

Once the vulnerabilities to an asset have been identified, a list of threat scenarios that take advantage of those vulnerabilities is developed. Again, this project focused on risks posed by terrorism, so all of the threat scenarios had to do with ways that terrorists might try to damage the assets in question.

By identifying the vulnerabilities of an asset and then developing threat scenarios based on those vulnerabilities, RFRM ensures that the security options developed in the risk management phases, which will be discussed later, are relevant to the asset in question.
Input from the VDOT site managers was again key for this part of the project. They were able to tell which scenarios were realistic and which were not. They were also able to give insight on potential scenarios that were not on the original list.

### 2.3 Filtering of Threat Scenarios

Phases III – V of RFRM involve filtering the threat scenarios in order to find the ones that are most severe and deserve the most attention. The scenarios are filtered qualitatively in Phase III using an ordinal risk matrix. This type of matrix was adapted from the U.S. Air Force’s Risk Matrix (Haimes, Kaplan, and Lambert, 389). This matrix shows the severity of a scenario by combining the likelihood of a given scenario occurring and the consequences of that scenario if it occurs. Figure 2 shows an example of this matrix. The bold line is the cutoff point for scenarios that will be filtered out and those that will be kept. Since the most severe scenarios are in the upper right-hand corner, any scenarios to the right of the line will be kept, and any to the left will be filtered out.

The way to place scenarios in this matrix is by asking the following question: “Given that someone will try to attempt a given scenario, what is the likelihood of its success?” This allows the scenario to be placed in one of the vertical columns that represent likelihood. The scenario must then be placed in one of the horizontal rows, which is done by determining what the most likely worst effect will be. For example, if a scenario can cause loss of life, it doesn’t matter whether it will cause short-term or long-term loss of mission because loss of life supercedes those two outcomes.

![Figure 2: Example of Ordinal Risk Matrix](image)

Phase IV of RFRM continues the filtering that was started in Phase III. This phase of filtering is again qualitative, but it now takes into account a set of 11 criteria that were developed by Haimes, Kaplan, and Lambert: undetectability, uncontrollability, multiple paths to failure, irreversibility, duration of effects, cascading effects, operating environment, wear and tear, hardware/software/human/organizational, complexity and emergent behaviors, and design immaturity (Haimes, Kaplan, and Lambert, 389). These criteria were considered when ranking the scenarios in this phase.

This phase of RFRM uses a specific set of criteria, but it is still qualitative even though it might seem like the criteria could be weighted and given numerical values in order to come up with a formula that would give a quantitative measure of the severity of the scenario in terms of the 11 criteria. This is because the developers of RFRM decided that giving weights to the criteria would make it too easy to manipulate the numbers to make them do whatever the user wanted. Therefore, these criteria are simply considered when filtering the scenarios.

Phase V of RFRM is quantitatively filtering the scenarios that remain after Phases III and IV. This is done using a cardinal matrix, which is just like the one shown in Figure 2, only with quantitative probabilities in the likelihood column instead of qualitative measures of risk. Like Phases III and IV, this process involved talking with the VDOT site managers to get their opinion on what would be the most dangerous threats to a site.

However, for this project, it was found that Phase V was not always necessary because in some cases, Phases III and IV did a sufficient job of filtering the scenarios down to a reasonable number. Also, for willful threats and terrorism scenarios, developing a quantitative risk matrix can be difficult due to the uncertainties involved.

All of this filtering allows the user to identify the scenarios that deserve the most attention. This becomes important when RFRM moves into the risk management phases because the user then is not wasting his attention on extraneous things.

### 3 RISK MANAGEMENT

#### 3.1 Evaluating Risk Management Options

The first phase of the risk management is Phase VI, in which risk management options are generated and evaluated. The options are generated by considering the list of filtered risk scenarios from the risk assessment. Management options are generated then in two categories; to prevent the risk scenarios and to respond to the risk scenarios. Five to ten preventative and five to ten responsive management options are developed and then evaluated.

The first step of the evaluation process involves first estimating the costs of implementing the options. Cost estimation can stem from one of two sources: expert input or vendor estimates. The eight case studies relied almost solely on estimates provided by VDOT personnel.
The cost should form a triangular distribution with a high cost, low cost, most likely cost, and then a subsequent expected value for cost. Furthermore, the cost estimates should take into account installation, operation, and maintenance costs. An example of a chart containing such costs is Table 1.

Table 1: Sample Table of Security Options Costs

<table>
<thead>
<tr>
<th>OPTION NUMBER</th>
<th>LOW COST</th>
<th>MEDIUM COST</th>
<th>HIGH COST</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>$60,000</td>
<td>$80,000</td>
<td>$100,000</td>
</tr>
<tr>
<td>2</td>
<td>$77,880</td>
<td>$80,000</td>
<td>$86,000</td>
</tr>
<tr>
<td>3</td>
<td>$113,520</td>
<td>$122,000</td>
<td>$146,000</td>
</tr>
<tr>
<td>4</td>
<td>200,000</td>
<td>$250,000</td>
<td>$300,000</td>
</tr>
<tr>
<td>5</td>
<td>$50,000</td>
<td>$72,000</td>
<td>$760,000</td>
</tr>
</tbody>
</table>

The next step in evaluating the management options is to determine their effectiveness. Effectiveness is determined according to the following criteria:

1. Reliability
2. Maintainability
3. Durability
4. Availability
5. Usefulness

Each option is first assigned a rank in terms of its effectiveness by a site expert.

The smaller the numerical value of the rank, the higher the effectiveness, and the more effective the option is in either preventing or responding to a terrorist attack. Then the options are assigned percentages to show the percent effectiveness they provide. The percentages for preventative options show the percent risk reduction by the implementation of the preventative option. The percentages for responsive options show the percent of overall damage and loss (including loss of life) that is prevented by the response to an attack, provided by the implementation of the responsive option. Furthermore, the estimated percent effective values allow the decision-maker to compare differences in effectiveness, which ranking alone fails to provide. An example of a chart with the effectiveness values for management options is shown in Table 2.

Table 2: Sample Table of Security Options Ranks and Effectiveness Ratings

<table>
<thead>
<tr>
<th>OPTION NUMBER</th>
<th>RANK</th>
<th>PERCENTAGE</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>#3</td>
<td>15%</td>
</tr>
<tr>
<td>2</td>
<td>#4</td>
<td>6%</td>
</tr>
<tr>
<td>3</td>
<td>#1</td>
<td>40%</td>
</tr>
<tr>
<td>4</td>
<td>#2</td>
<td>35%</td>
</tr>
<tr>
<td>5</td>
<td>#5</td>
<td>4%</td>
</tr>
</tbody>
</table>

3.2 Selecting Optimal Options

The next step in phase VI is multi-objective tradeoff analysis where Pareto-optimal graphs are plotted separately for preventative and responsive options. A Pareto optimal, or non-inferior, option, is an option where one objective can only get better at the expense of another objective getting worse. Discarding inferior options leads to no options being considered that are worse at both objectives.

The first step in determining Pareto-optimality is to graph the following two plots:

1. Median cost vs. Rank
2. Median cost vs. Percentage

Examples of the two charts explained above are contained in Figures 3 and 4.

Each point on the graph represents an option. The options along the Pareto optimal frontier (i.e. the line) are non-inferior as can be seen by comparing the 3rd ranked option to the 2nd ranked option, which is both less expensive and more effective. Therefore, a decision-maker would no longer consider the 3rd ranked option. All other inferior options are also filtered off. The decision-maker
should only consider Pareto optimal options for actual implementation.

3.3 Finishing Risk Management

Phase VII then follows where all previous phases are reviewed to ensure that no critical risk scenarios were overlooked by the management filtering process. The process is reviewed using the input of various stakeholders to ensure no critical elements have been omitted or overlooked. Appropriate adjustments are then made accordingly.

The final phase of the risk management is phase VIII where operational feedback is provided regarding the security options that have been implemented. Changes can be made as necessary. This underscores the fact that RFRM is an ongoing process that recognizes that situations can change and that adaptations must be made. However, for this project, none of the proposed security options have been implement, so Phase VIII was irrelevant.

4 FINDINGS

The analysis below can be considered successful on many levels. First, Hierarchical Holographic Modeling (HHM) lends itself to the creation of a robust and nearly definitive model of a given asset. Second, the risk scenarios generated successfully cover the spectrum of feasible terrorist attacks on a given asset. Third, the filtering process successfully limited the number of scenarios to consider for risk management to a reasonable set. Fourth, the management options generated creatively met the needs of a given asset. Fifth, the cost-benefit analysis successfully produced a small set of Pareto optimal management options.

Problems, nevertheless, arose in the project. The following are problems arising through the implementation of the RFRM methodology:

1. The subjective nature of risk assessment provides for an inherent dose of variability.
2. The filtering process gave undue credit to bombing scenarios that are unlikely to be given major consideration by decision-makers due to the immense cost needed to pay for appropriate protection.
3. The current set of consequences is somewhat limiting. The Capstone group determined that it would be beneficial to divide the “loss of life” consequence into “loss of life and 100% inoperability” and “loss of life and partial inoperability” so as to better separate risk scenarios.
4. The Capstone group determined that it would be easier for experts to consider a given management option’s effectiveness as opposed to having to determine who much a given option would reduce risk.
5. Eliciting cost estimates from vendors or VDOT personnel is difficult. Greater communication with VDOT will be needed in all future research.

Nonetheless, the project’s results are informative and beneficial. The project discovered common vulnerabilities and common management options to meet these vulnerabilities. The following are some common findings pertaining to nearly all transportation assets:

1. Power is vital to the functioning of an asset and must be protected.
2. CCTV is a very effective management option.
3. Basic fencing acts as an effective deterrent.
4. Alternative routes must be acknowledged and functioning at all times.
5. Lighting should be improved at all sites.
6. Standard visitor protocols need to be developed for all of VDOT assets.
7. Extensive contractor background checks are necessary to help deter any terrorist infiltration. Furthermore, all contractors should be monitored during their visit to any given site.
8. VDOT should look at all positions currently filled by contractors and determine whether there would be a significant benefit to making those positions VDOT jobs.
9. Evacuation protocols for each site need to be developed and documented.
11. All VDOT personnel should have a secondary communication line (e.g. cell phone) available to them in the case of emergency (e.g. power outage or terrorist attack).

A greater emphasis should be placed on recovery and response measures in any future research. Possible recovery and response measures include:

1. Increase the number of emergency phones and/or fire extinguishers on the premises.
2. Increase the number of security guards on duty.
3. Increase the number of emergency response signs.

5 CONCLUSIONS

The analysis above can be considered successful on many levels. First, the HHM is a robust and nearly definitive model of the tunnel system. Second, the risk scenarios generated successfully cover the spectrum of feasible terrorist attacks on the tunnel. Third, the filtering process successfully limited the number of scenarios to consider
for risk management to a reasonable set. Fourth, the management options generated creatively met the needs of the each asset. Fifth, cost-benefit analysis successfully produced optimal sets of management options.

Of course, problems arose in the project. The subjective nature of risk assessment provides for an inherent dose of variability. Furthermore, the filtering process gave undue credit to bombing scenarios that are unlikely to be given major consideration by decision-makers due to the immense cost needed to pay for appropriate protection.

Nonetheless, the project’s results are informative and beneficial. In addition, the results above do not merely benefit the eight assets studied. Rather, the results will be used in the development of a computer-based risk management tool. The similarities between the successes and failures of each case study will be acknowledged in the design of the tool. This program will enable VDOT personnel to enter data on their respective sites and generate a list of Pareto optimal management options. Thus, it relieves the burden of research necessary to generate such options. VDOT can then further investigate the options it will consider for use.

Needless to say, this tool is necessary in our modern world. Successful terrorist attacks have crossed national borders and entered our homeland. Our safety, both personal and economic, demands effective risk assessment and risk management. Hopefully this research will be a small, but lasting step towards greater public safety.

REFERENCES


AUTHOR BIOGRAPHIES

Elizabeth Jones is a fourth-year Systems and Information Engineering major from Midlothian, VA, concentrating in management. Her major contribution to the project was studying two important bridges: a double-swing-span bridge which frequently opens for the Navy as well as a bridge in a major urban center.

John Lyford, V is a fourth-year Systems Engineering major and Economics minor from Baton Rouge, LA. His major contribution to this project was studying a major interstate interchange asset and an Intelligent Transportation System (ITS) asset. Mr. Lyford will be commissioned as a 2nd Lieutenant in the U.S. Air Force in May and will proceed to pilot training, where he will train to become an Air Force pilot.

Mikail Qazi is a 4th year Systems and Information Engineering major from Islamabad, Pakistan. His major contribution to the project was the case studies on a major bridge and a major bridge–tunnel. Mr. Qazi will pursue a career in systems analysis after graduation.

Nicholas Jon Solan is a 4th year Systems Engineering student at the University of Virginia. He contributed case studies on a major interchange and tunnel system within Virginia. Mr. Solan will study environmental law after graduation.

ACKNOWLEDGEMENTS

The Capstone Group would like to thank following people for their contributions:

VDOT personnel, iSteven Mondul, Wayne Ferguson, John Bishop’, Andy Fowler, Steve Titunik, Kamal Suliman, and Amy Tung-McElwain; UVA graduate students Peach Leung, Alex Mosenthal, and Josh Stafford; Secretary Della Dirickson, and all the undergraduate programmers