An Application of Enterprise Risk Management in the Marine Transportation Industry

[1]M. D. Abkowitz, [2]J. S. Camp
[1,2]*Department of Civil and Environmental Engineering, Vanderbilt University, USA*

Abstract

Establishing the current status and future direction of an organization's enterprise risk management (ERM) practice demands an ability to benchmark the existing level of performance and prioritize where risk mitigation actions are warranted. This requires a systematic and holistic approach that can identify and assess every "reasonably foreseeable risk", compare risks on a common basis for prioritization of "hot spots", and evaluate the effectiveness of candidate risk mitigation strategies. Designing and implementing a management tool that organizations can utilize for this purpose is challenging, given that it must be comprehensive in nature, yet easy to apply.

This paper describes the development of such a tool and its subsequent application to a large marine transportation carrier. In this application, two separate ERM activities were undertaken; one focusing on a functional line of operations throughout the entire organization (information technology and cyber security), and the other involving all activities associated with a specific geographical region that serves as an operations hub. The resulting risk scenarios, assessments and candidate mitigation strategy evaluations are described and discussed.

The paper also shares several lessons learned that are important for organizations interested in developing and applying ERM tools. These include how to overcome the challenges of: (1) structuring a framework for identifying enterprise risks and creating corresponding scenarios that are all inclusive, (2) creating an appropriate system for associating the likelihoods and consequences with various risk scenarios, and (3) developing a protocol to enable evaluation of the benefits and costs of potential risk mitigation strategies that are developed in

response to those risks that have been deemed to warrant priority attention. Each of these challenges was encountered in the marine transportation carrier study.

Keywords: enterprise risk management, marine transport, cyber information security, risk identification, scenario analysis, risk mitigation, risk assessment, hazard analysis, disaster management

1 Introduction

Risk management has existed for centuries, beginning as far back as the *Code of Hammurabi* [1]. Today, in light of a spate of recent natural disasters, large-scale accidents and malicious acts, enterprise risk management (ERM) has become a favorite expression among organizations in both the private and public sector. Consequently, many organizations have instituted what they believe to be ERM as part of daily operations. Gates and Hexter [2], in surveying 271 financial and risk executives, reported that over one-half of respondents (56%) are making efforts to develop and implement some form of "enterprise risk management" strategy within their organizations, with another 35% of those surveyed positively disposed towards using ERM. Corporate governance, regulatory requirements, and an increased understanding of strategic and operating risks are motivating ERM implementation in these organizations [3].

While many firms are utilizing the term enterprise risk management, their approaches range from managing risks for a specific purpose to a company-wide implementation involving the commitment of considerable financial and human assets [4, 5]. In reality, it is only the holistic approach, one that includes all risk-related elements, hazards and scenarios, internal and external to the firm, which deserves the ERM label.

Central to any risk management activity is risk identification, which historically, has been heavily influenced by known problems or prior incidents. This reactionary mode typically limits the amount of creative thought that is invested in identifying all potential scenarios of what could go wrong. One popular approach to overcome this deficiency is to identify risks through compartmentalization, where each process, department or organizational group is viewed as a unique entity [6, 7]. Other approaches abound, such as those that categorize risk in terms of the recipient, whether it be workers, customers, the community, the environment, or an organization's physical assets [8].

While there may be variation in identification and categorization approaches, most importantly there is general agreement that enterprise risks encompass a variety of considerations, both within and external to an organization, affecting numerous stakeholders. This is an encouraging sign in terms of the potential for creating a holistic decision-support framework that can serve as the basis for establishing an ERM practice for any organization.

2 ERM Decision-Support Framework

In the work described herein, an ERM decision-support framework designed to address the aforementioned considerations is put forward for discussion and

applied in a case study environment. It is comprised of the following sequential steps.

1. Using risk and hazard categories, develop scenarios representing reasonably foreseeable events
2. Assign likelihood and consequence values (risk scores) to each scenario
3. Estimate annual "risk costs" and conduct absolute & comparative analyses
4. Identify and evaluate risk mitigation strategies

A more detailed explanation of each of these steps appears below.

2.1 Scenario Development

The task of developing appropriate scenarios begins with the definition of a set of ERM risk categories that is holistic in nature, but can be segmented into specific risk areas that are intuitively appealing and practical to apply. Table 1 presents the structure developed for this purpose.

Table 1: Enterprise Risk Categories

Internal	External
1. Operational	1. Operational
a. Product/Service Quality	a. Social, Political & Economic Relations
b. Employee/On-Site Contractor Relations	b. Customer, Supplier, and Off-Site Contractor Relations
c. Financial Management	c. Malicious Acts
2. Information Systems	2. Information Systems
a. Technology\Hardware & Software	a. Technology\Hardware & Software
b. Proprietary & Personal Information Management	b. Proprietary & Personal Information Management
3. Physical	3. Physical
a. Facility Infrastructure & Physical Assets	a. Infrastructure, Transportation, & Resource Availability
b. Employee Health & Safety	b. Environmental & Natural Hazards
c. Environmental Releases	

At the top level of the hierarchy, risk categories are defined first by whether they are considered internal or external in nature. The terms "internal" and "external" identify the origin of the hazard with respect to the organization in addition to providing an indication of the extent to which an organization can control the referenced risk. Some risk categories can be associated with both internal and external risks; however, the hazards that fall into these categories would be different. For example, an information security breach that originates as a computer virus sent by an email to an employee would be considered an external risk, whereas an employee copying files or stealing proprietary company information for personal gain would be considered an internal risk, even though both events involve information breaches that compromise the organization's intelligence and data systems.

Beyond the division of internal and external risks, risk categories are segmented into three principal dimensions: (1) operational, (2) information systems, and (3) physical. Operational risks are defined as those that relate to how business is transacted within the organization. These include risks associated with financial decisions, resource management, and relationships with employees, contractors and customers. Information system risks include computer hardware and software, as well as all "intangible" assets associated with those systems (i.e., data, employee personal information, bank records, and customer accounts). Among an organization's physical assets are buildings, stock and equipment. Employees and their wellbeing (i.e., health and safety) also falls into this category, along with those risks associated with environmental releases by the organization or by others (external) that may adversely impact business operations.

Within each risk category reside a number of different hazards that can threaten the organization. For example, in the External – Physical – Environmental & Natural Hazards category, hazards could include events such as tornadoes, earthquakes, floods, wildfires and heavy snowfall. Because the events associated with each hazard will differ, it is important to capture these circumstances in terms that can easily be envisioned for consideration and analysis. The most promising format for doing so is development of event scenarios for each hazard.

To fully understand the potential risks associated with each hazard, multiple scenarios must be evaluated. These scenarios should represent the range of events that are "reasonably foreseeable" that an organization may experience. The basis for determining these event scenarios is based on answering the question, "What could go wrong?" To capture the full breadth of possibilities, the developed scenarios should represent incremental levels of impact severity, ranging from events with minor to catastrophic outcomes. Referring to the previous discussion, for a tornado hazard, at one end of the spectrum, a scenario might be a tornado warning for a two-hour window during the business day where the organization is situated, although a tornado does not subsequently materialize. On the other end of the scenario spectrum might be a direct hit to the facility by an F4 tornado that completely destroys the building and causes

human casualties. Of course, other scenarios can be constructed to represent tornado events that fall in between these extremities.

What is critical at this stage is that all reasonably foreseeable risks have been identified and characterized in the form of scenarios for each hazard in each of the risk categories. Therefore, as the risk assessment process progresses, one has confidence that the organization will experience no surprises because it was systematic and comprehensive in how it approached risk identification.

2.2 Risk Scoring

To evaluate the risk associated with each scenario, two important components must be taken in consideration: 1) the likelihood (frequency) that the scenario could occur and 2) the consequences if the scenario does occur.

Recognizing that there will typically be a large number of scenarios and limited availability of loss prevention data, this necessitates a scoring system that can elucidate reasonable responses to these two risk inputs. As a result, the semi-quantitative risk scoring method shown in figure 1 was developed. The first scale in figure 1 corresponds to establishing scenario likelihood. Note that the selection options range from occurrences expected to be extremely rare to those that may happen several times within a given year. If a Level 1 or Level 5 frequency is assigned to a scenario, then a supplemental table is provided that enables the user to become more precise with their frequency estimate (e.g., 1 in 100-year event; daily event).

The bottom two scales in figure 1 are used for consequence estimation. Here, property/asset impacts are separated from those that describe impacts to human health. The reason for this segmentation is that participants engaged in this process typically consider property/asset impacts on a monetary scale, whereas impacts to human health are more commonly quantified in terms of fatalities and injuries. Although there is a desire to combine all impacts into a single economic unit, that computation is done later as an internal feature that is derived from available “value of statistical life” literature [9, 10].

Frequency

Level	1	2	3	4	5
	Extremely Rare	Rarely	Occasionally	Annually	Semi-annually
Description	Occurs less than once in 25 years	Occurs less than once every 10 years, but more than once every 25 years	Occurs less than once every 5 years, but more than once every 10 years	Occurs less than once every 5 years, but more than once per year	Occurs at least once per year, but less than once per month.

Consequence - Impacts on Property/Assets

Level	1	2	3	4	5
Description	Minimal	Moderate	Significant	Severe	Catastrophic
	Between $0 and $100	Between $100 and $1,000	Between $1,000 and $10,000	Between $10,000 and $100,000	Over $100,000

Consequence - Impacts on Human Health

Level	1	2	3	4	5
	Minimal	Moderate	Significant	Severe	Catastrophic
Description	Persons are treated on site for minor injuries and released, if any impact at all	Level 1 plus one or more persons requiring emergency room treatment	Level 2 plus one or more persons requiring hospitalization	Level 3 plus fatalities of 1 to 5 persons	Level 3 plus fatalities of more than 5 persons

Figure 1: Risk Scoring Method Scales

2.3 Risk Analysis

Using the results from the previous step, an estimated "risk cost" can be computed by multiplying the scenario likelihood by its corresponding economic consequences. A convenient way to report this information is on an annual basis, which is simply derived by converting likelihood into annual terms (i.e., an event that is expected to occur once every 25 years is assigned an annual likelihood of 0.04) and then multiplying it by the event consequence cost.

There are two popular ways to present these results. One is a table showing the annual risk cost for each scenario. The other is in the form of a "heat map", essentially a graph where one coordinate represents the scenario likelihood and the other represents the economic consequence. We find both approaches to be useful in understanding the risks associated with each scenario. Whereas the table allows for a rank ordering in purely economic terms, the heat map provides insight into whether a scenario with a significant risk cost is being driven by a high probability, low consequence event or a low probability, high consequence event. This has ramifications when it comes to applying resources to risk mitigation both in terms of priority and expenditure.

Evaluation results can be aggregated to the decision-maker's level of interest, with the scenarios being the most detailed level. At some point, it will be important to compile the risk scores for all scenarios in a hazard class, so that the risk associated with different hazards can be compared (e.g., Is my risk greater for tornadoes or earthquakes?). At an additional level of aggregation, risk scores can be compared among different categories (e.g., Am I more exposed to

employee health and safety risk or natural hazard risk?). Finally, at the highest level of aggregation, the total risk cost for the enterprise in a given year can be established. This provides a means for examining the vulnerability of the organization as a whole, while also serving as a baseline against which to measure progress as mitigation strategies are implemented.

2.4 Mitigation Strategy Evaluation

The identification and evaluation of risk mitigation strategies is a bit more complicated than one might imagine. While it is logical to focus development and deployment of mitigation strategies on those scenarios, hazards, and/or risk categories that represent the largest economic burden to the organization, a couple of important considerations may prevail. First, not every mitigation strategy will necessarily produce a sufficient reduction in risk cost to justify its investment. Secondly, many mitigation strategies will offer risk reduction benefits that accrue across multiple scenarios, hazards and risk categories. As a result, a structured assessment process is needed.

To address these considerations, an economic benefit cost analysis approach using net present value was adopted. The implementation costs associated with a prospective mitigation strategy can be estimated in a straightforward manner, assuming adequate information on capital and operating costs, investment lifetime and discount rate. However, deriving the economic benefit (i.e., reduction in risk cost) requires returning to the scenarios where the mitigation strategy in question is intended to reduce scenario risk, either by diminishing likelihood, consequence or both. In each of these instances, the decision-maker is asked to re-score under the assumption that the candidate mitigation strategy has been implemented. The net change in risk cost from original scoring and then re-scoring is used as the benefit metric in determining the value of the proposed mitigation strategy. Of course, it is up to the decision-maker to determine whether the associated benefit/cost meets a threshold for strategy investment.

3 Case Study Application

The methodology, as previously described, was applied to a large marine transportation carrier. In this application, two separate ERM activities were undertaken; one focusing on a functional line of operations throughout the entire organization (information technology and cyber security), and the other involving all activities associated with a specific geographical region that serves as an operations hub.

3.1 Scenario Development and Scoring

The scenario development process involved working directly with company executives to identify risk categories and hazards that the organization faces, including what could go wrong in each instance. Care was given to define a set

of scenarios that ranged from those likely to produce relatively benign impacts to those with the potential for catastrophic outcomes. A particular challenge was to limit the number of scenarios such that participants would not find the scoring process to be burdensome without sacrificing coverage of relevant risks. Once the scenarios were defined, participants were asked to score the scenarios using the scales presented in figure 1.

3.2 Risk Analysis Results

Risk analysis results for the IT and cyber security application appear in table 3, expressed in annual risk cost. Only those hazards with annual risk costs in excess of $1 million are shown, an arbitrary threshold for presentation purposes. Note that leakage of employee, customer and proprietary data dwarfs the others in terms of annual risk cost, representing a problem in excess of $10 million a year. The rationale behind this concern is that if business confidential information falls into the hands of a competitor, this can have a significant impact on the company's competitive edge and therefore its bottom line. The annual frequency of occurrence is estimated to be quite high for most scenarios falling into this hazard category (see heat map in figure 2), perhaps an indication of how recent WikiLeaks activity has exposed the vulnerability of information espionage.

Hazards with annual risk costs in excess of $1 million are shown in table 4 for the operating region application. This is accompanied by figure 3, which presents a heat map showing scenarios associated with external malicious acts, the hazard deemed as having the largest annual risk cost for the operating region. Of particular interest in reviewing this heat map is that the overall annual risk cost is driven almost exclusively by Scenario 4, a situation in which a gunman or explosive device renders considerable harm to people located in the facility, resulting in multiple fatalities and injuries. This low probability, but high consequence event can be evaluated by a risk manager as either being too remote a possibility to worry about, or a situation where the consequences could threaten the very existence of the business. Depending on this perspective, reducing this risk could be a high priority or not warrant much attention.

Table 2: Risk Analysis Results – IT and Cyber Security

Hazard Categories		Annual Risk Costs ($)
Tier 1 - Greatest Risk (Greater than $10M)		
	Cyber - Information Leakage (Employee, Cust., and Proprietary Data)	$14,802,000
Tier 2 - High Risk ($2.5M - $10M)		
	Networks - Unauthorized Access/Security Breach (PC)	$4,630,000
	Physical - Snow	$3,264,000
	Software - Upgrades (Failure or Lack Thereof)	$3,232,000
Tier 3 - Moderate Risk ($1M - $2.5M)		
	Networks - Network Failure or Crash (Internet)	$2,113,000
	Cyber - Backups/System Redundancy Failure	$2,014,000
	Physical - Fire (Forest, Range, Wildland)	$1,969,000
	Physical - Tornado or Strong Winds	$1,947,000
	Hardware - Denial of Service/Usage (System Shut Down or Crash)	$1,866,000
	Physical - Earthquake	$1,865,000
	Cyber - Information Theft (Employee, Customer, and Proprietary Data)	$1,854,000
	Cyber - Website Hacking	$1,553,000
	Physical - Hurricane/Tsunami	$1,422,000
	Physical - Offices	$1,137,000
	Networks - Internet Abuse (Band Width, Illegal Sites, etc.)	$1,112,000

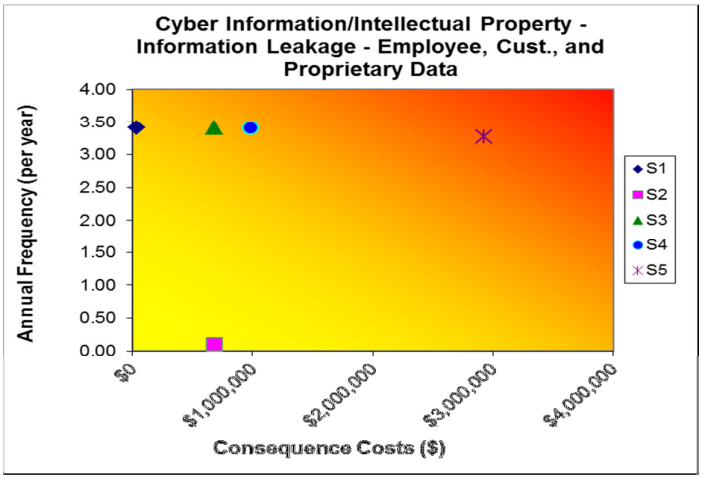

Figure 2: Employee, Customer and Property Data Leakage Scenario Heat Map. S1 - An associate sets up an email rule to automatically forward received email to a personal email account of theirs or others. S2 - A system is set up to forward email to non-corporate domain email accounts (e.g., Gmail, Yahoo). The individual receiving the email leaves the organization and joins a competitor, yet continues to receive the former organization's email, which may be confidential business. S3 - An associate copies information to a personal device (e.g., memory stick, USB drive) for purposes of using the information for business on their home computer. This device is not encrypted and is inadvertently

lost. S4 - An associate discovers information of value on a system or report, and shares that information with friends or relatives for their personal gain. S5 - An associate bypasses the corporate data retention policy for email, documents, etc. and makes unauthorized electronic or hard copies.

Table 3: Risk Analysis Results - Operating Region

Hazard Category		Annual Risk Costs ($)
Tier 1 - Greatest Risk (Greater than $10M)		
	N/A	--
Tier 2 - High Risk ($2.5M - $10M)		
	External - Malicious Acts - Terrorist or Disgruntled Employee	$4,536,000
	Internal - Information Systems - Internet Abuse	$4,012,000
Tier 3 - Moderate Risk ($1M - $2.5M)		
	External - Physical - Tornado or Strong Winds	$2,373,000
	Internal - Physical - Employee Health (Slip, Trip, Fall)	$2,133,000
	External - Physical - Impaired Air Quality	$1,942,000
	External - Economic - Market Conditions	$1,640,000
	Internal - Physical - Facility Damage (Random Incident)	$1,210,000

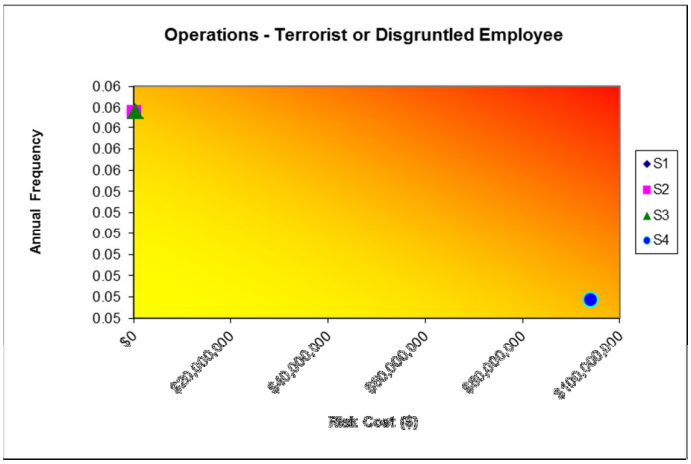

Figure 3: Malicious Act by Terrorist or Disgruntled Person Scenario Heat Map. S1 - You have recently fired an employee who the organization viewed as violent and emotionally unstable. S2 - Your facility or one adjacent to yours receives a letter threatening a bomb attack or release of a chemical or biological agent; OR an employee receives a package that contains a white powder. S3 - A small explosive device or mildly toxic chemical/biological agent is discharged or released inside your facility or a nearby facility. The device/chemical impacts a portion of your facility. S4 - Employees in your facility are being held hostage

by a gunman and shots have been heard OR an explosive device is discharged inside your facility that causes serious damage.

One area of interest is the extent to which a functional line within an organization and the employees who utilize that resource view the same risks. Figure 4 displays the annual risk costs for IT hazards that were common to both the IT functional line and the operating region. Note that in most instances, the party responsible for the resource (the IT group) recognized the significance of certain risks that were considered rather benign by the operating region. This is not surprising given that many of these hazards are integral to the functional line's services and may not be transparent to the end user. However, in one instance, internet abuse, the disparity in the opposite direction is striking. One could surmise that the IT department has underestimated the amount of internet abuse practiced by employees on a routine basis. This underscores the need to involve multiple stakeholders in the ERM process so that both awareness and risk score accuracy are enhanced.

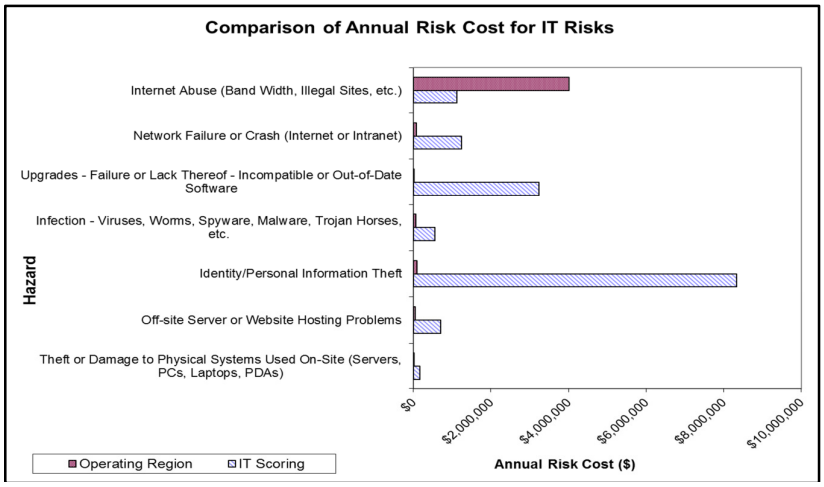

Figure 4: Comparison of IT and Operating Region Responses

3.3 Mitigation Options Evaluation

Deployment of the mitigation strategy benefit-cost analysis is underway. Although results cannot be reported as yet, the approach is outlined below.

Participants are being asked to use the risk analysis results to determine the importance of mitigating risks belonging to certain categories, hazards and scenarios. This spawns a set of mitigation strategies worthy of evaluation. The process for determining the benefit-cost of each candidate strategy is illustrated

in table 5. Three prospective mitigation strategies are shown (enhance emergency evacuation plan; improve firewalls and security; implement weather warning system), along with their respective annual implementation cost. The net risk cost reduction from re-scoring is shown within the table by strategy and hazard. The total risk cost reduction, when aggregated across all relevant hazards, represents the overall strategy benefit. The benefit-cost ratio is then computed. Note that, in this illustration, strong justification exists to implement improved firewalls and security, whereas the other two strategies are unlikely to justify further consideration.

Table 4: Illustration of Mitigation Strategy Benefit Cost Analysis

			Risk Cost Reduction ($)					
	Mitigation Options	Implementation Cost ($)	Cyber Info Leakage	Networks - Unauthorized Access	Physical - Snow	Physical - Flood	Total Risk Reduction ($)	B/C Ratio
M1	Enhanced Emergency Evacuation Plan	$100,000			$10,000	$40,000	$50,000	0.50
M2	Improved Firewalls and Security	$2,000,000	$5,000,000	$240,000			$5,240,000	2.62
M3	Weather Warning System	$750,000			$150,000	$200,000	$350,000	0.47

3.4 Discussion

The case study applications yielded several observations regarding implementation of the ERM framework which are currently being used to revise the methodology. They include the following:

1. To gain cooperation and focus from participants, it is important to limit the number of scenarios for consideration.
2. Scenario descriptions must be carefully reviewed for accuracy and ease of understanding prior to their use.
3. The number of levels in scoring tables should be limited so as to elucidate differences in likelihood and consequences without being overly precise.
4. Respondents should be allowed to designate “Do Not Know” so that arbitrarily assigned scores do not bias the evaluation outcome.
5. When possible, likelihood and consequence scores should be quality-controlled by assessing “reasonableness of results” relative to empirical loss data.
6. When large differences in individual scores occur for the same scenario, an attempt should be made to reconcile the disparity.
7. Having a sufficient number of participants involved in the scoring process is essential to achieving representative results.

4 Conclusions

An ERM methodology has been devised and field-tested whose design is to capture all reasonably foreseeable risks using a protocol that is considered practical and achievable. Results to date indicate that it can serve as a valuable tool, provided that care is given to how risk categories, hazards and scenarios are defined, the manner in which scenario likelihood and consequence is estimated, how the results are interpreted, and the process from which mitigation strategies are developed and assessed. Our research is continuing to refine the methodology and to expand its use to other organizations, both in the private and public sector.

6 Acknowledgements

This research was sponsored by the Intermodal Freight Transportation Institute at the University of Memphis through the federal Safe, Accountable, Flexible, Efficient Transportation Equity Act: A Legacy for Users (SAFETEA-LU). The authors are grateful for this support as well as the assistance provided by employees of the marine transportation carrier described herein.

References

[1] Covello, V.T. and J. Mumpower, *Risk Analysis and Risk Management: An Historical Perspective.* Risk Anlaysis, 1985. **5**(2): p. 103-120.

[2] Gates, S. and E. Hexter, *The Strategic Benefits of Managing Risks.* MIT Sloan Management Review, 2005.

[3] Gates, S., *Incorporating Strategic Risk into Enterprise Risk Management: A Survey of Current Corporate Practice.* Journal of Applied Corporate Finance, 2006. **18**(4): p. 80-91.

[4] Lam, J., *Enterprise-wide Risk Management and the Role of the Chief Risk Officer.* ERisk.com, 2000: p. 1-5.

[5] Nocco, B.W. and R.M. Stulz, *Enterprise Risk Management: Theory and Practice.* Journal of Applied Corporate Finance, 2006. **18**(4): p. 8-20.

[6] COSO, *Enterprise Risk Management - Integrated Framework.* . 2004, New York, NY: Committee of Sponsoring Organizations of the Treadway Commission (COSO), American Institute of Certified Public Accountants .

[7] EPCB, *Complete Continuity Toolkit. EPCB Risk Management Consultants*, www.emergencyriskmanagement.com

[8] Trammell, S.R., D.K. Lorenzo, and B.J. Davis, *Integrated hazards analysis.* Professional Safety, 2004. **49**(5): p. 29-37.

[9] Viscusi, W.K. and J.E. Aldy, *The Value of a Statistical Life: A Critical Review of Market Estimates Throughout the World.* Journal of Risk and Uncertainty, 2003. **27**(1): p. 5-76.

[10] Eeckhoudt, L.R. and J.K. Hammitt, *Background Risks and the Value of Statistical Life.* Journal of Risk and Uncertainty, 2001. **23**(3): p. 261-279.