An Analysis of Transportation Security Risk Regulation Regimes: Canadian Airports, Seaports, Rail, Trucking and Bridges

Kevin Quigley, PhD
School of Public Administration
Dalhousie University
Halifax, Nova Scotia
Corresponding Author
E-mail: kevin.quigley@dal.ca

Bryan Mills, Dalhousie University

February 1, 2014

DALHOUSIE UNIVERSITY
Inspiring Minds

Acknowledgments

This paper is the result of a research project on critical infrastructure protection that started in 2008. We have conducted research on the transportation, manufacturing (dangerous chemicals) and agricultural sectors. The authors wish to acknowledge the support of the Social Sciences and Humanities Research Council (Standard Operating Grant No. 410-2008-1357; Partnership Development Grant No. 890-2010-0123), Public Safety Canada and the Kanishka Project Contribution Program. The views expressed in this paper do not necessarily reflect the views of the Government of Canada.

Special thanks also go to the 75 interview subjects (50 of whom were interviewed for this paper) from four countries who graciously gave their time in support of this research. We also wish to acknowledge the several graduate students at Dalhousie University who have assisted in this research since its inception. Many of the 2011 and 2012 interviews were conducted and transcribed by Emily Pond. This document was copy-edited by Janet Lord. A late draft of the paper was reviewed by Professor Mary R. Brooks, transportation specialist at and Adjunct Professor, Graduate Studies, Dalhousie University.

While we are grateful for the support from these sources, the authors alone are responsible for any errors or omissions.

Table of Contents

1.0 Executive Summary 1
What We Found 1
What We Recommend 7
Future Research 8
Sommaire Exécutif 9
Ce Que Nous Avons Découvert 10
Ce Que Nous Recommandons 17
Des Recherches à Venir 17
2.0 Introduction 19
Definitions and Limitations 19
3.0 The Framework 22
3.1 Applying the Framework: Content 23
3.1.1 Airports 23
3.1.2 Seaports 26
3.1.3 Trucking and Rail 28
3.1.4 Bridges 33
3.2: Interdependencies: All Subsectors 35
4.0 Risk Regulatory Regime: Context 37
4.1 Market Failure Hypothesis 37
4.2 Opinion-Responsive Hypothesis 42
4.3 Interest Group Hypothesis 49
5.0 Conclusion 56
5.1 Appendix I: Methodology 57
5.2 Appendix II: Interview Participants 59
5.3 Appendix III: List of Selected CI events for Media Analysis 61
5.4 Appendix IV: Cultural Theory Summary 62
5.5 Appendix IV: Notes about the Authors 63
6.0 Works Cited 64

List of Tables and Figures

Figure 1: Hood, Rothstein and Baldwin (2001): Understanding Risk Regulation Regimes 22
Figure 2: Responses from aviation interview participants to the question: "How would you rate the influence of the following subjects on how you spend your time with respect to matters of safety and security?" 25
Figure 3: Responses from port interview participants to the question: "How would you rate the influence of the following subjects on how you spend your time with respect to matters of safety and security?" ... 28
Figure 4: Responses from rail interview participants to the question: "How would you rate the influence of the following subjects on how you spend your time with respect to matters of safety and security?" ... 32
Figure 5: Responses from trucking interview participants to the question: "How would you rate the influence of the following subjects on how you spend your time with respect to matters of safety and security?" 33
Figure 6: Responses from bridge interview participants to the question: "How would you rate the influence of the following subjects on how you spend your time with respect to matters of safety and security?" 35
Figure 7: Responses from interview participants to the statement: "On which of these sectors do you rely the most to ensure successful operation of your business?" 36
Figure 8: Market failure explanation of regime size. 38
Figure 9: Responses from participants to the question: On a scale of one to ten, in which ten means 'very confident' and one means 'not confident at all', how confident are you in your business continuity plans following this event?'. 39
Figure 10: Three public opinion polls: Do you think it is … that Canada will be the victim of a major terrorist attack in the next two years? (Environics Institute, 2002, 2004, 2006) 43
Figure 11: All hazards: Government performance assessment and volume of coverage in print media by event type (Australia, Canada, UK, U.S.) 45
Figure 12: Cultural Theory typology 50

Table 1: Voluntary certification programs 29
Table 2: List of Interview participants 59
Table 3: List of interview participants by sector and type 60
Table 4: List of selected CI events for media coverage analysis 61

List of Acronyms

BM	Behaviour modification
CPA	Canada Port Authority
CAA	Canadian Airport Authority
CN	Canadian National
CP	Canadian Pacific
CI	Critical Infrastructure
CIP	Critical infrastructure protection
CTPAT	Customs-Trade Partnership Against Terrorism
FAST	Free and Secure Trade
IG	Information gathering
INT	Interview
MFH	Market failure hypothesis
PIP	Partners in Protection
RAC	Railway Association of Canada
RAP	Rational actor paradigm
SMS	Safety Management System
SME	Small and medium-sized enterprises
SS	Standard setting

1.0 Executive Summary **(French Language Executive Summary Follows)**

We employ the Hood, Rothstein and Baldwin (2001) meso-level risk regulation regime framework to conduct an analysis of Canadian transportation security in these five subsectors: airports, seaports, rail, trucking and bridges. First, we describe and analyse the information-gathering, standard-setting and behaviour-modification practices of these subsectors with respect to security. Secondly, we explore the context that potentially influences the risk regulation regimes, including the role of markets, public opinion/media and organized interests.

We conducted 50 semi-structured interviews between 2011 and 2013 with regulators, owners, operators, managers and representatives of critical transportation infrastructure. Most interview subjects work for Canadian organizations, although we also interviewed specialists from Australia, the UK and the U.S. to provide some comparative perspective. The interview tool and process were approved by Dalhousie University's Research Ethics Board. We also conducted a review of the academic and grey literature and a media analysis of 24 post-9/11 critical infrastructure (CI) events, four of which primarily affected the transportation sector.

The paper is an overview of security and (to a lesser extent) safety practices in a necessarily vast and complex sector; the paper is not meant to be an exhaustive account of security practices in Canadian transportation. Rather, we want to put this new interview and media data in the public domain, first, to contribute to a better understanding of the present security challenges and opportunities within the sector, and secondly, to prompt further thinking and research in this area. The content section (Section 3.1 to 3.2), in particular, relies significantly on the perspective of those working within the sector and those regulating it. Primary constraints on the research include the scope of the transportation sector (from local to global), the difficulty in obtaining reliable security data, the limited amount of time to conduct the research, the limited number of interview subjects and the inevitable limitations of human perspective (researcher and interview subjects). Finally, the interviews occurred at some point over the last three years. People's views change and adapt. As best as we could, and notwithstanding the use of the framework, we let the interview transcripts speak for themselves.

What We Found

Regime Content

This regime content section summarizes our principal observations concerning information-gathering, standard-setting and behaviour-modification practices in security in each of the five subsectors we studied.

Interview subjects at **airports** feel that information gathering for airports is largely cooperative and collaborative among key stakeholders. There are clear, albeit extensive standards for

security, which are developed largely by Transport Canada in consultation with industry as well as a number of other national and international organizations. Transport Canada is active in enforcing behaviour modification at airports, resulting in a robust—although rules- and process-oriented—control mechanism for the subsector. Legal and policy concerns exert considerable influence on airport staff. Some interview subjects note that the regime is at times too inflexible and does not take the unique characteristics of each airport into account. Interview subjects expressed the most concern over risks associated with terrorism.

Compared to airport staff, **seaport** staff feel that information gathering is not as collaborative or cooperative; standards and behaviour modification are driven by getting products to market as quickly as possible. Interview subjects think there has been insufficient effort to examine the sector as a whole and evaluate, for example, vulnerabilities caused by interdependencies. Overall, port staff face a number of competing contextual pressures and are less satisfied than airport staff with the regulatory regime. Interview subjects expressed the most concern over risks associated with climate change and extreme natural events.

In **trucking**, information gathering seems less restricted by formal rules and is less consistent, more dispersed and intermittent. Standards vary across locations, and behaviour modification depends on private incentives, laws and, sometimes, membership in voluntary organizations. Interview subjects noted that the trucking industry is influenced most by markets and their legal dynamics, including meeting customer needs, insurance concerns and government road regulations. Interview subjects expressed the most concern over risks associated with cargo theft and major collisions causing service disruption.

In the **rail** sector, government and industry interactions are influenced largely by the three Class 1 rail companies, which are exposed to varying degrees of competitive pressure; safety concerns receive more attention than security ones. For small and medium-sized enterprises (SMEs), there is a reliance on the local law enforcement community and rail associations for information and standards regarding security risks. Railway staff identified regulations and media coverage as influencing them the most when it comes to safety and security and how they spend their time. When it comes to security, in particular, interview subjects expressed the most concern over risks associated with terrorism and public access points to rail infrastructure.

Bridges are unique in the transportation sector in that they are fixed infrastructure that is effectively monopolistic. Staff share information and best practices with staff from other bridges. While there is a strong regulatory regime in place for safety, security is less formal and based largely on shared best practises and relationships with local law enforcement and staff at other bridges. Bridge staff identified engineering risks and media coverage as influencing them most when it comes to safety and security and how they spend their time. Bridge staff expressed the most concern over risks associated with severe weather events.

Regime Context

This section summarizes three contextual pressures—markets, public opinion/media and organized interests—that potentially influence the information-gathering, standard-setting and behaviour modification techniques within the risk regulation regime.

Markets

Different types of ownership—from public to private—will dictate the degree of direct influence government has over the security of CI. The transportation sector is complex, and in fact, government does not have direct control over the vast majority of the critical transportation infrastructure. The owner of the infrastructure is not common across the subsectors we studied. The largest seaports and airports are owned by the federal government but managed via a lease or concession, or corporatized commercial entity; smaller facilities may be owned by other orders of government or private companies. In trucking, ownership of the vehicles is widely fragmented while the largest share of the infrastructure used (both roads and bridges) is government-owned and -maintained, although there are some private roads and bridges. As for rail, the ownership is privately held by the railroads, while, in some cases, there are running rights held by public companies like VIA or private cargo owners.

While most sectors are regulated when it comes to safety and security, market structures vary considerably in the critical transportation infrastructure, which will impact the kinds of risks the subsectors face and the size, structure and style in which the regulatory regimes operate. Some subsectors are competitive (trucking) while others are monopolistic (bridges); some are heavily regulated (airports) while others have more flexibility (trucking); some are regulated primarily by one order of government (bridges, airports and seaports) while others are regulated by several (rail and trucking); some subsectors have considerable redundancies and are adaptive (trucking) while most have critical elements that are static/immovable and include high-consequence single-points of failure (seaports, airport, rail and bridges).

In addition, security threats vary depending on the subsector, location and connection to international trade, and can range from those which capture the public's attention, such as terrorism, drug smuggling, people trafficking, people smuggling, to those which have perhaps more serious business implications, such as piracy, cargo theft and cyber risks, to the more mundane and probable, such as trespassing and petty crime. Many risks relate to broader questions of the underground economy in Canada, economic and political stability in parts of the developing world and access to key trade routes in international markets. There are also vulnerabilities to safety generated by communicable diseases, aging infrastructure, natural disasters and human error. The necessary openness and accessibility of public transportation also creates safety and security threats.

It is difficult to justify the costs of standing at the ready for such a multitude of low-probability events. The complexity and uncertainty (Renn, 2008) of the risk, the associated problem of

holding someone to account for the failure of complex and interdependent systems, the cost of reducing risk exposure and the importance of CI to our collective well-being combine to reduce the incentives for any one individual company, and particularly cash-strapped small and medium-sized enterprises (SMEs), to act in advance of any CI events. Security is almost always seen as a negative expense. In this sense, the market fails to protect against disasters to which the public has a strong aversion and for which communities can pay a high economic and social cost.

Consequently, governments will likely have a strong role to play in the risk regulation regime, including in collecting, validating and disseminating information. Timely and actionable intelligence can allow CI owners, operators and managers to adapt according to their own needs and circumstances. Such an approach works best if everyone's interests are aligned and key players are prepared to share information; this is not always the case. Depending on the subsector and indeed the organization, several factors can influence the extent to which organizations may be willing to share information, including competition, incentives, penalties, confidence, willingness, perceived importance of the information, concern over leaks, authority, organizational culture, market sensitivities, ownership and capacity, for example.

In any event, government must go beyond information-gathering. Governments must ensure adequate standards are in place; strong standards can convey best practices, increase transparency, facilitate coordination and clarify accountability. Excessively high standards can also dull competitive advantage if implemented without adequate industry consultation. As a result, strategies intended to change organizations' behaviour must encompass a broad, multi-faceted approach, and range from stick-and-carrot tactics, such as financial incentives, penalties and lawsuits to softer tactics, such as education, collaboration and diplomacy. In order to be effective, the strategies must incorporate incentives and softer techniques that are appropriate to the specific subsector (as outlined in the Interests section (4.3) of this paper and summarized below) as well as recognize how the affected organizations connect to the specific goals and broader mission of the transportation sector as a whole.

Media and Public Opinion

Public opinion can be volatile; the literature on the psychology of risk provides many insights into the potentially irrational and erratic reaction people have to risk events and CI failures. Many interview subjects also noted the influence of the media on how the interview subjects spend their time in relation to safety and security concerns; rail and bridge staff cited the media as one of their top concerns. Low-probability/high-consequence events generate high-volume media coverage for a concentrated period of time. Different types of events—natural disasters, industrial failures, terrorist plots, cyber events, for example—generate different types of coverage, not just in volume but in tone and in their search for accountability. Different subsectors also generate different types of coverage. The volume of media coverage does not necessarily relate to the consequence (as measured in dollars) or probability of a disaster. While the public will almost always expect government to be involved at some level in the response to

these events, our research suggests media coverage can vary dramatically from being supportive of government and public services (some natural disasters and failed terrorist plots) to blaming them (industrial failures) to indifference (cyber, with the possible exceptions of on-line child exploitation and insider threats). Finally, after a disaster, and for a short period of time, media and public opinion (however volatile) come into play with greater force. Arguably, this disrupts the normal control mechanisms and creates opportunities for change, which under normal circumstances are often resisted by many of the dominant interests.

This change in dynamic can present opportunities to overcome entrenched interests and also problems with handling over-reactions. Focussing on highly emotive issues (and neglecting more probable risks) can generate attention and motivate change for a limited period but can also lead to narrow and misguided risk assessments. More complete information in the public domain, which addresses knowledge gaps on an on-going basis, can help to mature the public's (and the media's) opinion on security issues and CI events, and in so doing offset the likelihood and consequences of over-reaction.

Interests

A study of organizational culture helps to identify different forms of governance and their associated strengths and weaknesses. Each subsector has unique characteristics, which generate different preferences. We apply a Cultural Theory framework to analyze the five subsectors. The theory measures regulation and social integration to determine value systems and the preferred institutional arrangements flowing from them, leading to the characterization of four types: hierarchists, individualists, egalitarians and fatalists. We do not claim our categorizations of these five subsectors are absolute but rather suggest that certain organizational traits become more apparent in subsectors when we place all five in comparative perspective. This allows us to identify potential strengths and weaknesses in each subsector, and also the potential organizational differences between subsectors that undermine coordination across the transportation sector as a whole. While the framework was useful in organizing a discussion of the subsectors in comparative perspective, the limited availability of reliable security data makes it difficult to be conclusive.

We employ the framework as a heuristic device to orient our thinking and provide an opportunity for further analysis and questioning. Within this framework, we categorize:

- Airports and rail organizations as hierarchical (high regulation / high integration), which suggests a focus on expertise, forecasting and management but their size can make them sluggish and routine-driven and they can struggle with outward accountability. Their strength lies in their potential for strong leadership, stability, extra human and financial resources and ability to secure expertise. To enhance security practices, hierarchical organizations should work on flexibility, adaptive capacity, transparency and organizational learning.

- Seaports as fatalists (high regulation / low integration), which are isolated and do not feel in control of their circumstances. Fatalists are skeptical, which can be a strength when others claim their systems are robust, resilient and impenetrable. Security practices can be enhanced by integrating the seaports more fully into the security community of practice; this will require increased trust, transparency and knowledge exchange between key interests.
- Bridge organizations as egalitarian (high integration / low regulation), which focuses on team dynamics at the expense of broader engagement. Egalitarians can be highly committed to their team identity and responsibilities; information exchange is low-cost due to the size, informality, similar training and non-competitive nature of the team. Security practices can be enhanced by encouraging greater communication and outward accountability with interests *outside* of the transportation sector and emergency services, and a more formalized approach to security.
- Trucking as individualist (low integration / low regulation), which is atomistic and focuses on private incentives and market signals at the expense of the collective good and group coordination. Provided there are appropriate incentives, individualists are highly adaptive which is crucial and rare in the transport sector due to the fixed nature of most critical transportation infrastructure. Security practices can be improved by strengthening the incentive structure for security; this will be more successful if security is demanded from their customer base, not regulated by government. Government might also work closely with the trucking industry groups to understand how to collect more reliable information from a sector that is highly dispersed and how best to coordinate it during a CI event.

All five subsectors can benefit from scenario planning that tests their ability in non-routine events.

In addition to highlighting the potential strengths and weaknesses of different forms of governance, Cultural Theory underscores that one must bring a more nuanced understanding of each subsector to the fore when attempting to regulate risks. Policy initiatives should play to each subsector's strengths but also be aware of their weaknesses and, in fact, set policies to moderate these weaknesses. In some cases, this might require manipulation of the two key variables: increase/decrease regulation and increase/decrease integration. Blanket transportation policies across all subsectors are unlikely to be interpreted and enacted in a consistent manner. Given these fundamental tensions between subsectors, the theory also prompts questions about the view that the transportation system works as a unified whole, and raises concern about the vulnerabilities that emerge in coordinating across the subsectors in light of a major CI event.

Concluding Comments

Standing at the ready for low-probability/high-consequence events can rarely be justified in market terms. We find that when subsectors experience less competition and regulatory

complexity and stronger incentives and organizational commitment to enact security, security practices are more robust. In many instances, however, security competes with a number of market and cultural/institutional pressures.

At the same time, it is a highly volatile policy space. The media amplify disasters and the public has a fascination with them and aversion to them. In this sense, having a strong information-gathering capacity in place is a necessary but not adequate condition for government regulatory regimes. As critical infrastructure is essential to our collective social and economic needs, government must develop—however deftly—capacity for enacting standards and behaviour change without being an excessive regulatory burden on these sectors. Emphasizing best practices in business continuity in each subsector, for example, will likely generate more traction in the business community than focussing too much on specific low-probability events. Progress on transparency, accountability, prioritization, redundancy and adaptive capacity will help, as will a strong sense of purpose guided by liberal democratic values. The approach will be more effective if underpinned by an understanding of the unique contextual and institutional influences in each subsector, and how the subsector interacts with and supports the specific goals and the broader mission of the transportation sector as a whole.

What We Recommend

There are a number of recommendations throughout this report. Based on our research, we believe the following subjects constitute our principal recommendations and require additional research and regulatory attention.

- With respect to security, ensure regulators have adequate capacity across the three components of a cybernetic control model: information gathering, standard setting and behaviour modification. Behaviour modification tends to be the most difficult to achieve and requires a mix of incentives, penalties and persuasiveness. The approach must be backed by clear accountability and appropriate levels of transparency. Practices must be informed by the unique context of each subsector.
- Further integrate the seaports and trucking sectors into the security community. Ports require further institutional integration into the government's security apparatus; trucking requires a better incentive structure and organization.
- Examine and strengthen incentive structures for CI sectors and particularly SMEs to develop more robust business continuity plans, including formal agreements with key suppliers and adequate insurance coverage, when possible.
- Draw from the more commonly accepted safety practices to initiate stronger security practices.
- Enhance transparency and outward reporting on the state of CI to the citizenry.

Despite the unique characteristics of each of the subsectors and the segmented bureaucratic organizations that regulate them, the transportation sector ideally must function as a unified

whole. We need a better understanding of how the unique characteristics of each subsector disrupt the seamless interaction between these subsectors, and what policies, practices and institutional arrangements can help to overcome these deficiencies.

Future Research

The following concepts did *not* come up very often in our interviews but were frequent themes at academic and professional conferences and in the academic and grey literature. We highlight these themes here because they represent potential threats and opportunities for the transportation sector; further investigation would benefit the sector.

- How municipalities can use their big data more effectively to ensure a more resilient response to emergencies.
- How small and medium-sized enterprises address business continuity planning and insurance needs, and the resulting vulnerabilities.
- How governments can coordinate small and medium-sized enterprises during crises.
- How the transportation sector is addressing risks associated with insider threats.
- How the transportation sector is addressing cyber threats.
- The opportunities and security threats associated with increased Arctic trade routes.
- How the transportation sector manages risks associated with terrorist threats towards sectors upon which the transportation sector is heavily reliant, namely finance and energy.
- How the unique characteristics of each subsector undermine the effective and efficient functioning of the transport sector as whole, and what policies, practices and institutional arrangements can help to address these weaknesses.
- Finally, our interview tool did not explicitly ask about the impact of climate change, however, interview subjects, particularly in seaports, raised this as a top-of-mind risk.

Sommaire Exécutif

Nous employons le cadre d'applications Hood, Rothstein et Baldwin (2001) du régime méso-échelle pour l'atténuation des risques pour entreprendre une analyse de la sécurité des transports au Canada dans ces cinq sous-secteurs : les aérogares, les ports de mer, les voies ferroviaires, le camionnage, et les ponts. Au départ, nous décrivons et analysons les pratiques qui gouvernent la collecte d'informations, l'établissement de normes et la modification du comportement en rapport avec la sécurité dans ces sous-secteurs. Ensuite, nous explorons le contexte qui aurait une influence potentielle sur ces régimes qui régularisent les risques, y compris le rôle joué par les marchés, l'opinion publique/médiatique et les intérêts organisés.

Nous avons entrepris 50 interviews semi-structurées entre 2011 et 2013 avec des régulateurs, des propriétaires, des gestionnaires et des représentants d'infrastructures essentielles dans le domaine des transports. La majorité de nos sujets pour ces interviews travaillent pour des organisations canadiennes, par contre nous avons aussi interviewé des spécialistes venant de l'Australie, du Royaume-Unis et des États-Unis pour offrir une perspective comparative. Les outils et les méthodes pour ces interviews ont reçu l'approbation du Conseil de déontologie dans les recherches de l'Université Dalhousie. De plus, nous avons aussi entrepris une révision de la littérature grise, de la documentation parallèle et une analyse médiatique de 24 événements d'infrastructures essentielles (IE) post 9/11, dont quatre qui touchent plus particulièrement le secteur Transport.

Cet article sert comme vue d'ensemble de la sécurité et (à un degré inférieur) des méthodes de sécurité dans ce qui est nécessairement un secteur vaste et complexe; l'intention n'est pas de présenter un rapport exhaustif des méthodes de sécurité dans le secteur Transport au Canada. Nous cherchons plutôt à introduire dans le domaine public ces nouvelles données médiatiques et ces interviews, premièrement pour contribuer à une meilleure compréhension des défis actuels ainsi que les opportunités présentes à l'intérieur du secteur, et ensuite, pour encourager une réflexion plus approfondie accompagnée de recherches plus poussées dans le domaine. La partie Contenu (section 3.1 à 3.2), plus précisément, dépend de façon importante sur la perspective de ceux qui travaillent à l'intérieur du secteur et ceux qui le régularisent. Les contraintes majeures pour ce qui est des recherches comprendraient l'étendu du secteur Transport (du local au mondial), la difficulté qu'il y a à obtenir des données fiables sur la sécurité, le temps limité pour entreprendre cette recherche, le nombre limité de sujets à interviewer et les restrictions inévitables de la perspective humaine (recherchistes et sujets interviewés). Et finalement, ces interviews se sont échelonnées sur une période de trois ans. Les points de vue et les opinions changent et évoluent. Autant que cela nous a été possible, nonobstant l'emploi de l'infrastructure, nous permettons aux transcriptions de parler pour eux-mêmes.

Ce Que Nous Avons Découvert

Contenu du Régime

Ce secteur sur le contenu du programme résume nos principales observations quant à la collecte de données, l'établissement de normes et les pratiques pour la modification du comportement dans le domaine de la sécurité dans chacun des cinq sous-secteurs que nous avons étudiés.

Les sujets interviewés dans les **aérogares** estiment que la collecte d'informations dans les aérogares est en grande partie due à une collaboration et une coopération parmi les principaux intervenants. Il y a en place des normes très claires, quoique généralisées, pour la sécurité, qui sont développées en grande partie par Transport Canada en consultation avec l'industrie aussi bien qu'avec d'autres organismes nationaux et internationaux. Transport Canada s'active à faire l'application de la modification du comportement aux aérogares, avec comme résultat un mécanisme de contrôle robuste--bien qu'axé sur la poursuite des règlements-et du processus--pour le sous-secteur. Les inquiétudes politiques et légales exercent une forte influence sur le personnel des aérogares. Quelques sujets interviewés notent qu'à certains moments le régime devient inflexible et ne tient pas compte des caractéristiques uniques de chaque aérogare. Les sujets interviewés ont exprimés davantage d'inquiétudes face aux risques associés avec le terrorisme.

À la différence du personnel d'aérogare, le personnel de **ports de mer** a le sentiment que la collecte d'informations n'est pas aussi collaborative ni coopérative; les normes et la modification du comportement sont sous l'impulsion d'amener les produits aux marchés aussi rapidement que possible. Les sujets interviewés pensent qu'il y a déficience d'efforts à examiner le secteur en entier et à évaluer, par exemple, les interdépendances. Dans l'ensemble, le personnel de ports de mer fait face à un certain nombre de pressions contextuelles et ces travailleurs sont moins satisfaits que le personnel d'aérogare avec le régime régulateur. Les sujets interviewés ont exprimé leurs plus grandes inquiétudes face aux risques associés au changement climatique ainsi que les évènements naturels extrêmes.

Pour ce qui est du **camionnage**, la collecte d'informations semble moins restreinte par les règles formelles et elle est moins consistante, plus dispersée et plus intermittente. Les normes varient selon les lieux, et la modification du comportement dépend de l'initiative privée, des lois, et parfois, de l'adhésion à des organismes volontaires. Les sujets interviewés ont noté que l'industrie du camionnage est surtout influencée par les marchés et leurs dynamiques légales, y compris les demandes du client, les inquiétudes face aux assurances ainsi que les règlements routiers gouvernementaux.

Les sujets interviewés ont exprimés leurs plus fortes inquiétudes face aux risques associés avec le vol du cargo et les collisions majeurs causant des perturbations de service.

Dans le secteur **ferroviaire**, les interactions du gouvernement et de l'industrie sont influencées en majeure partie par les trois Classe1 des compagnies ferroviaires, lesquelles sont exposés à des degrés différents de pressions compétitives, bien que les inquiétudes sur la sûreté reçoivent davantage d'attention que celles sur la sécurité. Pour les petites et moyennes entreprises (PME), il y a une confiance dans l'exercice des pouvoirs des forces policières communautaires ainsi que les associations ferroviaires afin d'obtenir les informations et les normes vis-à-vis les risques de sécurité. Le personnel ferroviaire a identifié les règlements et la couverture médiatique comme étant les sources qui les influencent le plus en ce qui concerne la sûreté et la sécurité ainsi que l'usage de leurs temps. En ce qui concerne la sécurité, en particulier, les sujets interviewés ont exprimé leurs plus fortes craintes à propos des risques associés au terrorisme ainsi qu'aux points d'accès pour le grand public à l'infrastructure ferroviaire.

Les **ponts** sont uniques dans le secteur Transport en ce qu'ils sont une infrastructure fixe et qui est monopolistique. Le personnel partage l'information ainsi que les meilleures pratiques avec le personnel de d'autres ponts. Bien qu'il existe un régime régulateur puissant en place pour la sûreté, la sécurité est moins formelle et elle est basée fortement sur l'échange des meilleures pratiques et les liens avec la police locale et le personnel de d'autres ponts. Le personnel de pont a identifié les risques en génie ainsi que la couverture médiatique comme influence majeure en ce qui les concernent le plus en rapport avec la sûreté et la sécurité et l'usage de leurs temps. Le même personnel exprime leurs plus grandes appréhensions en ce qui concerne les risques associés aux des évènements de température violente.

Contexte du Régime

Cette section résume trois pressions contextuelles--les marchés, l'opinion publique/médiatique et les intérêts organisés--qui influencent potentiellement la collecte d'information, la normalisation et les techniques de modification du comportement à l'intérieur du régime de réglementation des risques.

Les Marchés

Les différents types de droits de propriété--du publique au privé--vont dicter le degré d'influence directe que le gouvernement peut avoir sur la sécurité IE. Le secteur Transport est complexe, en fait, le gouvernement n'a pas de contrôle direct sur la vaste majorité de l'infrastructure critique au transport. Le propriétaire de l'infrastructure n'est pas le même à travers les sous-secteurs que nous avons étudiés. Les plus gros ports de mer et aérogares sont la propriété du gouvernement fédéral mais ils sont gérés par un bail ou une concession, ou encore par une entité commerciale corporative; des installations plus petites peuvent être la propriété de d'autres secteurs du gouvernement ou de compagnies privées. Dans le camionnage, la propriété des véhicules est largement fragmentée, pendant que la vaste majorité de l'infrastructure utilisée (et les routes et

les ponts) est la propriété du gouvernement et maintenue par lui, bien qu'il y a certaines routes ou même des ponts privés. Pour ce qui est du transport par rail, c'est la propriété privée des chemins de fers, tandis que dans certains cas, certains droits de circulation sont détenus par des compagnies publiques, comme par exemple VIA, ou des propriétaires de cargo privés.

Tandis que la plupart de ces secteurs sont réglementés lorsqu'il est question de sûreté et de sécurité, les structures de marché varient considérablement dans les infrastructures critiques du Transport, ce qui a des répercussions sur le genre de risque auquel les sous-secteurs font face et cela en plus de la taille, la structure et le style dans lequel les régimes régulateurs opèrent. Certains sous-secteurs sont compétitifs (le camionnage) tandis que d'autres sont monopolistiques (les ponts); certains sont fortement réglementés (les aéroports) alors que d'autres sont plus flexibles (le camionnage); certains sont règlementés principalement par un seul décret de gouvernement (les ponts, les aéroports, et les ports de mer) alors que d'autres le sont par plusieurs (le rail et le camionnage); certains sous-secteurs ont une redondance considérable et sont adaptatifs (le camionnage) tandis que la plupart ont des éléments critiques qui sont statiques/stationnaires et qui incluent des points de défaillance singuliers à hautes conséquences (les ports de mer, les aérogares, le rail, et les ponts).

En plus, les menaces à la sécurité varient dépendant du sous-secteur, la localisation, leur relation au commerce international, et peuvent varier de ce qui peut capter l'attention publique, tel que le terrorisme, la contrebande de drogues, le trafic de personnes, le trafic de migrants, à ceux qui sans doute ont des implications d'affaires plus sérieuses, comme la piraterie, les vols de cargo, les cyber-risques, jusqu'au plus banals et probables, tel que l'intrusion, et le crime mineur. Bien des risques sont reliés à la question plus générale de l'économie souterraine au Canada, la stabilité politique et économique dans certaines parties du monde en développement et l'accès à des routes de commerce clés dans les marchés internationaux. Ils existent aussi certaines vulnérabilités à l'égard de la sûreté générées par les maladies transmissibles, le vieillissement de l'infrastructure, les désastres naturels ainsi que l'erreur humaine. La transparence obligatoire et l'accessibilité au transport publique créent aussi des menaces à la sûreté et la sécurité.

Il est difficile de justifier le coût de cette position de se tenir toujours prêt devant une si grande multitude d'événements peu probables. La complexité et l'incertitude (Renn,2008) des risques, le problème associé au fait de prendre à partie quelqu'un dans le cas d'une défaillance de systèmes complexes et interdépendants, le coût d'une réduction à l'exposition au risque et l'importance des infrastructures essentielles à notre bien-être mutuel se réunissent pour décourager toute incitation pour toute entreprise particulière agissant seule, et surtout ces petites et moyennes entreprises à court d'argent (PME), pour agir en avance d'événements d'IE. On a presque toujours tendance à voir la sécurité comme un coût négatif. Et dans ce sens, le marché manque de se protéger contre les désastres pour lesquels le public à une forte aversion et pour lesquels les communautés paient une facture élevée autant sur le coté économique que social.

C’est pourquoi les gouvernements auront en toute probabilité un rôle essentiel à jouer dans ce régime régulateur qui vise à réduire les risques, y compris la collecte, la validation et la dissémination d’informations. Des renseignements opportuns et recevables pourraient permettre aux propriétaires d’IE, aux exploitants et aux gestionnaires de s’adapter selon leurs propres besoins et circonstances. Une telle approche réussira mieux si les intérêts à tous sont harmonisés et si les participants-clés sont prêts à partager les renseignements; ceci n’est cependant pas toujours le cas. Dépendant toujours des sous-secteurs et à vrai dire de l’organisation elle-même, plusieurs facteurs peuvent avoir une influence sur la bonne volonté des organisations à partager l’information, y compris la compétition, les schémas d’intéressement, les pénalités, la confiance, la volonté de collaboration, l’importance apparente de l’information, les inquiétudes au sujet des fuites, l’autorité, la culture entrepreneuriale, les sensibilités du marché, le droit de propriété et la capacité, par exemple.

De toute évidence, le gouvernement se doit de s’aventurer au-delà de la collecte d’informations. Les gouvernements doivent s’assurer que des normes appropriées aux risques soient en place; les normes supérieures peuvent indiquer les pratiques exemplaires, et ils peuvent augmenter la transparence, faciliter la coordination et clarifier la responsabilisation. Des normes trop élevées, si on les met en œuvre sans consultation adéquate avec l’industrie, peuvent nuire à la compétition. Comme résultat, les stratégies destinées à modifier le comportement des organisations doivent inclure une vaste approche à multiples facettes ainsi qu’une gamme de tactiques style la carotte et le bâton, tels que des stimulants financiers, des pénalités et procès civils aux tactiques plus douces, telles que l’éducation, la collaboration et la diplomatie. Pour être efficace, les stratégies doivent incorporer des mesures incitatives et des techniques plus douces qui sont appropriées pour ce sous-secteur spécifique (souligné dans la partie Intérêts de ce texte (4.3) et résumé ici-bas) aussi bien que de reconnaitre la façon dont ces organismes impliqués sont rattachés à des buts spécifiques et à la mission plus large du secteur Transport en tant qu’entité.

Les Medias et l’Opinion Publique

L’opinion publique peut s’avérer volatile; la littérature sur la psychologie du risque offre une connaissance approfondie des réactions potentiellement irrationnelles et erratiques que peuvent avoir les gens aux événements à risque et aux défaillances d’IE. Plusieurs sujets dans ces interviews avaient aussi noté l’influence des medias sur leur emploi du temps en relation avec les questions de sureté et de sécurité; ceux qui travaillent sur les ponts et les voies ferroviaires avaient cité les medias parmi leurs plus grandes inquiétudes. Les événements à faible risque et à conséquence élevée génèrent une grande couverture médiatique à haut volume sur une période de temps concentrée. Différents types d’évènements--les catastrophes naturelles, des échecs industriels, des complots terroristes, des cyberévénements, par exemple -- génèrent différents genres de couverture médiatique, pas seulement pour ce qui est du volume mais aussi dans leur tonalité et dans leurs recherches de ceux qui sont responsables. Différents sous-secteurs vont nécessairement générer différents types de couverture. Le volume de couverture médiatique n’est

pas nécessairement relié aux conséquences (pertes financières) ou à la probabilité d'un désastre. Pendant que le public s'attendra presque sans exception à ce que le gouvernement s'implique à un niveau ou l'autre pour répondre à ces événements, nos recherches suggèrent que la couverture médiatique peut varier de façon dramatique, d'un côté soutenant le gouvernement et les services ecollectifs (certains désastres naturels et complots terroristes manqués) mais de l'autre coté à les tenir responsables (désastres industriels) et de là jusqu'à l'indifférence (cyber, avec l'exception possible de l'exploitation d'enfants en ligne ainsi que les menaces internes). Finalement, suite à un désastre, et pour une courte période de temps, l'opinion des médias et du public (peu importe la volatilité) entre en jeu avec une plus grande force. On pourrait soutenir que cela interrompe les mécanismes normaux de control et peut créer des opportunités pour le changement, lesquelles, dans les circonstances normales, sont souvent évitées par les participants dominants.

Ce changement dans la dynamique peut présenter des opportunités pour surmonter les intérêts enracinés ainsi que pour traiter les problèmes de réactions excessives. La focalisation sur des questions émotives en litige (en négligeant les risques probables) peut générer une certaine attention et motiver pour le changement pour un temps limité mais peut aussi mener à des évaluations étroites et malavisées. De plus amples informations dans le domaine public, pour adresser de façon progressive les lacunes dans la connaissance, pourraient aider à faire évoluer l'opinion public (et celle des médias) sur les questions de sûreté et d'évènements d'IE, et ce faisant, contrebalancer la probabilité de réactions excessives et les conséquences excessives qui en résulteraient.

Intérêts

Une étude sur la culture organisationnelle aide à identifier différentes formes de gouvernance ainsi que leurs points forts et leurs faiblesses. Chaque sous-secteur a ses propres caractéristiques, ce qui génère des préférences variées. Nous employons l'infrastructure d'application d'une théorie culturelle afin d'analyser les cinq sous-secteurs. Cette théorie jauge l'intégration réglementaire et sociale afin de déterminer les systèmes de valeurs ainsi que les mesures institutionnelles préférentielles qui en découlent, menant à la caractérisation de quatre types; hiérarchique, individualiste, égalitaire, et fataliste. Nous n'insistons pas sur notre catégorisation de ces cinq sous-secteurs mais plutôt nous suggérons que certains traits organisationnels se font plus apparents dans les sous-secteurs lorsque nous plaçons ces cinq secteurs dans une perspective de comparaison. Ceci nous permet d'identifier les forces et faiblesses dans chaque sous-secteur et aussi les différences organisationnelles potentielles entre chaque sous-secteur qui minent la coordination à travers le secteur Transport dans son entier. Tandis que l'infrastructure avait son utilité dans l'agencement de discussion des sous-secteurs dans une perspective de comparaison, la disponibilité de données de sécurité fiables rend la tâche difficilement péremptoire.

Nous employons l'infrastructure comme instrument heuristique afin d'orienter notre façon de penser et prévoir une possibilité pour faire suite à l'analyse et l'interrogatoire. À l'intérieur de l'infrastructure, nous catégorisons:

- Les aérogares et le rail comme hiérarchiques (haute réglementation/haute intégration), qui suggère un focus sur les connaissances spécialisées, la projection et la gestion tandis que leurs taille peuvent les rendent anémique et dicté par la routine et ils peuvent se débattre avec l'obligation de rendre des comptes vers l'extérieur. Leur force est liée à leur potentiel pour un leadership robuste, à la stabilité, à un surplus de ressources humaines et financières en plus de l'habilité de sécuriser les compétences spécialisées. Afin de rehausser les pratiques de sécurité, les organisations hiérarchiques doivent travailler sur la flexibilité de leur capacité adaptive, sur la transparence et l'apprentissage de l'organisation.
- Les ports de mer comme fatalistes (haute réglementation/ intégration basse), sont isolés et ne se sentent pas en contrôle de leurs circonstances. Les fatalistes sont sceptiques, ce qui peut être une force lorsque d'autres prétendent que leurs systèmes sont robustes, résilients et impénétrables. Les pratiques de sécurité peuvent êtres rehaussées en intégrant plus pleinement les ports de mer dans une pratique de sécurité au niveau communautaire; ceci nécessite une confiance accrue, la transparence et l'échange de connaissances entre les parties intéressées.
- Les ponts comme égalitaires (haute intégration/ réglementation basse), qui se focalisent sur la dynamique d'équipe aux dépens d'une implication élargie. Les égalitaires peuvent être hautement engagés à leur identité d'équipe et leurs responsabilités; l'échange d'information est bon marché dû à leur taille, l'absence de formalisme, un apprentissage similaire et la nature non-compétitive des équipes. Les pratiques de sécurité peuvent être rehaussées en encourageant une plus grande communication et une obligation de rendre compte avec intérêts à *l'extérieur* du secteur Transport et des services d'urgences, ainsi qu'en ayant une approche à la sécurité plus formalisée.
- Le camionnage comme individualiste (intégration basse / réglementation basse), ce qui est atomistique et focalisé sur des mesures d'incitations privés et sur les invitations du marché et cela aux dépens du bien collectif et d'une coordination au niveau du groupe. Pourvu qu'il y ait des encouragements appropriés, les individualistes sont hautement adaptatifs, ce qui s'avère crucial et assez rare dans le secteur Transport, là où la majeure partie de l'infrastructure essentielle est de nature fixe. On peut améliorer les pratiques de sécurité en renforçant la structure à caractère incitatif pour la sécurité; ceci connaitra un plus grand succès si cette sécurité vient à la suite de demandes de la part de la clientèle, et non pas par une réglementation venant du gouvernement. Ce gouvernement pourrait aussi travailler étroitement avec les groupements dans l'industrie Transport pour bien comprendre comment procéder à une collecte de données plus fiables d'un secteur qui est très dispersé et aussi comment avoir une meilleure coordination pendant un événement d'IE.

Les cinq sous-secteurs pourraient tous bénéficier d'une planification de scenarios qui mettraient à l'épreuve leur capacité dans les événements irréguliers.

En plus de souligner les points forts et les déficiences dans les différentes formes de gouvernance, la théorie culturelle souligne aussi le fait qu'on doit apporter une compréhension plus nuancée de chacun des sous-secteurs lorsque l'on tente de réglementer les risques. Les incitations offertes doivent aller chercher les points forts de chaque sous-secteur mais doivent aussi demeurer conscients de leurs points faibles et, en fait, créer des politiques pour modérer ces faiblesses. Dans certains cas, ceci pourrait demander la manipulation des deux variables-clés: accroître-décroître la réglementation et accroître-décroître l'intégration. Il est peu probable que ces politiques généralisées du Transport à travers tous les sous-secteurs soient interprétées ou qu'elles soient adoptées de manière consistante. Étant donné ces tensions fondamentales entre les sous-secteurs, la théorie soulève aussi des questions concernant le coup d'œil que le système du transport présente comme entité unifié, et soulève de l'inquiétude à propos des vulnérabilités qui émergent dans la coordination à travers les sous-secteurs en vue d'évènements majeurs d'IE.

Commentaires Finales

Être prêt et toujours sur ses gardes pour des évènements de basse probabilité/haute conséquence peut rarement être justifié en termes de marché. Nous trouvons que lorsque les sous-secteurs connaissent moins de compétitivité et de complexités régulatrices et de plus forts schémas d'intéressement ainsi que des engagements organisationnels à promulguer la sécurité, les pratiques de sécurité sont plus robustes. En plusieurs cas, cependant, la sécurité fait compétition avec un nombre de pressions du marché ainsi que de nature culturelle/institutionnelle.

En même temps, c'est un milieu d'influence politique hautement volatile. Les médias amplifient les désastres et le public ressent une fascination ou une aversion envers de tels événements. Dans ce sens, avoir en place une forte capacité pour la collecte d'informations est nécessaire mais n'est pas une condition adéquate pour des régimes régulateurs gouvernementaux. Tandis qu'une infrastructure critique soit essentielle pour nos besoins collectifs, sociaux et économiques, le gouvernement doit développer--cependant de façon habille--la capacité d'adopter des changements de normes et de comportements, sans toutefois être une charge régulatrice excessive sur ces secteurs. Mettre en évidence les meilleures pratiques de continuité d'affaires plutôt que trop focalisé sur des évènements spécifiques à basse probabilité devrait générer davantage de traction dans la communauté d'affaires plutôt que de trop focaliser sur des événements spécifiques à faible probabilité. Faire du progrès pour ce qui est de la transparence, la responsabilisation, la priorisation, la redondance et la capacité adaptive aidera, aussi bien qu'un sens prononcé du but guidé par des valeurs démocratiques et libérales. L'approche sera plus efficace si elle est étayée par une compréhension des influences contextuelles et institutionnelles uniques dans chaque sous-secteur, et comment le sous-secteur interagit avec, et

comment il soutien, les buts spécifiques et la mission plus générale du secteur Transport dans son entier.

Ce Que Nous Recommandons

Il y a plusieurs recommandations à l'intérieur de ce rapport. Basé sur nos recherches, nous croyons que les sujets suivants constituent nos recommandations principales et requièrent de plus amples recherches et une attention régulatrice.

- Pour ce qui est de la sécurité, s'assurer que les régulateurs aient une capacité adéquate à travers les trois composantes d'un modèle de contrôle cybernétique: la collecte d'informations, le réglage des normes, la modification du comportement. La modification du comportement a tendance à être le plus difficile à atteindre et nécessite un ensemble de schémas d'intéressement, de pénalités et du pouvoir de persuasion. L'approche doit être soutenue par une responsabilisation claire ainsi que des niveaux appropriés de transparence. Les pratiques doivent êtres informées par le contexte unique de chaque sous- secteur.
- Intégrer davantage les ports de mer et les secteurs du camionnage au sein de la sécurité communautaire. Les ports de mer exigent davantage l'intégration institutionnelle à l'intérieure de l'appareil sécuritaire du gouvernement; le camionnage nécessite une meilleure structure de mesures incitatives et d'organisation.
- Examiner et renforcir les structures pour les mesures incitatives pour les secteurs d'IE et en particulier les PME pour développer des projets d'enchainement plus robustes, y compris des ententes formelles avec des fournisseurs-clés et avec les assurances à risque assuré si possible.
- Choisir parmi les pratiques de sécurité généralement acceptées pour initier des pratiques de sécurité plus robustes.
- Rehausser la transparence et les déclarations externes sur l'état d'IE à la population.

Malgré le caractère unique de chacun des sous-secteurs et les organismes bureaucratiques segmentés qui les réglementent, le secteur Transport doit fonctionner idéalement comme une entité unifiée. Il nous faut une meilleure compréhension de la façon que chacun de ces sous-secteurs avec ses caractéristiques uniques peut désorganiser l'interaction unifiée de ces sous-secteurs, et quelles politiques, quelles pratiques et quels arrangements institutionnels seraient utiles pour surmonter ces insuffisances.

Des Recherches à Venir

Les concepts suivants ne se sont *pas* présentés très souvent au cours de nos interviews mais ils étaient fréquemment présents comme thèmes dans les conférences professionnelles et académiques et dans la littérature grise. Nous faisons ressortir ici ces thèmes parce qu'ils

représentent des dangers et des opportunités potentiels pour le secteur Transports. Une étude plus approfondie pourrait avantager ce secteur.

- Comment les municipalités pourraient se servir de leurs données massives de manière plus efficace pour assurer une réponse plus résiliente aux urgences.
- Comment les petites et moyennes entreprises abordent la planification pour la pérennité de l'entreprise et pour les besoins dans le domaine de l'assurance, avec les vulnérabilités qui en résultent.
- De quelle façon les gouvernements pourraient coordonner les petites et moyennes entreprises durant les crises.
- Comment le secteur Transport répond aux risques associés à une menace interne.
- De quelle manière le secteur Transport répond aux cybermenaces.
- Les opportunités aussi bien que les dangers associés à la multiplication des routes de commerce dans la région arctique.
- Comment le secteur Transport gère les risques associés aux menaces terroristes envers les secteurs, tels la finance et l'énergie sur lesquels ils dépendent en large mesure.
- Comment les caractéristiques uniques à chacun des sous-secteurs peuvent miner le fonctionnement efficace et efficient du secteur Transport en tant qu'entité, et quelles politiques, solutions pratiques appliquées et quels arrangements institutionnels pourraient être utiles pour adresser ces faiblesses.
- Et finalement, notre enquête par entrevue n'a pas expressément abordé le sujet de l'impacte du changement climatique, cependant, les sujets, et plus particulièrement ceux qui résident dans les ports, avaient cité ceci comme un risque qui les préoccupe nettement.

2.0 Introduction

For the purposes of this paper we use Hood *et al.*'s (2001) meso-level Risk Regulation Regime framework to examine the security regimes in five subsectors of the Canadian transportation sector: airports, rail, seaports, trucking and bridges. The Hood *et al.* (2001) framework is sufficiently flexible in that it casts a wide net for an inductive approach: the framework considers the law, the market, the media, public opinion, interests and institutions when examining factors that are potentially critical to understanding governments' approaches to risk management. Moreover, the Hood *et al.* framework is a comparative tool, which allows us to compare subsectors within transportation.

Data for this paper is drawn from the transcripts of 50 semi-structured interviews with owners, operators, managers and regulators in the transportation sector that were carried out between 2011 and 2013. We also conducted a literature review and analyzed media coverage of 24 low-probability/high-consequence events, four of which affect the transportation sector in particular.

In sum, we first describe and analyse the information gathering, standard setting and behaviour modification of five subsectors within transportation with respect to security. Secondly, we explore the context that surrounds the risk regulation regimes, including the role of markets, public opinion/media and organized interests, in order to determine what influences the respective risk regulation regimes of these five subsectors.

Definitions and Limitations

Safety and Security

While this research is focussed largely on security, the concept of safety[1] also came up repeatedly in our interviews. We try in this paper to distinguish between the two but at times interview subjects conflated the subjects. Security risks involve human aggressors who are influenced by a variety of environmental and personal factors and may come from within or outside the target institution (Reniers and Pavlova, 2013: 8). While their outcomes may be similar, security and safety risks demand different approaches to risk management. "[P]rotecting installations against intentional attacks," write Reniers and Pavlova, "is fundamentally different from protecting against random accidents or acts of nature" (2013: 9; see also Russell and Simpson, 2010). Human aggressors, for example, are adaptive agents; they will modify their behaviour in light of security practices organizations adopt. Generally, safety plans tend to be more transparent, are informed by more reliable data and are regulated more clearly. Safety plans are also more clearly entrenched in the organizational culture and legal tradition of many critical sectors.

[1] To many people in the transport industry, safety is about lost workdays due to accident and fatalities as a result of work activities, and they pay a workers' compensation premium to address this.

Critical Infrastructure Protection

Critical infrastructure protection seeks to enhance the physical and cyber security of key public and private assets and mitigate the effects of natural disasters, industrial accidents and terrorist attacks. The Government of Canada has identified ten critical sectors. Most Western governments have similar—though not identical—lists for their countries. The UK government has identified nine sectors and the U.S. government has identified 18, for example.

Critical Transportation Infrastructure in this research paper

In this paper we examine airports, seaports, trucking, rail and bridges. Because of the complex and necessarily interdependent nature of the sector, interview subjects occasionally conflated notions of airports with airlines, for example. While these related concepts come up occasionally, this paper does not include as a primary focus airlines, shipping or other key surface infrastructures, such as pipelines, buses or subways.

Risk and Regulation

Risk is a probability, though not necessarily calculable in practice, of adverse consequences (Hood *et al.*, 2001). Regulation means attempts to control or mitigate risk, mainly by setting and enforcing product or behavioural standards (Hood *et al.*, 2001). Risk regulation is governmental intervention with market or social process to influence and control to varying degrees potential adverse social and economic consequences.

Limitations to this Research

The corresponding author is a public administration specialist. He uses qualitative methods, including semi-structured interviews, and a broad range of social science literature, including references from psychology, political science, sociology and anthropology, to study governance and risk. We are not transportation specialists, per se. We used the Hood *et al.* framework to design the interview tool and analyze the data. We interviewed regulators and owners, operators and managers of CI, and, notwithstanding the framework, we did our best to let the data speak for itself. We use some commonly applied concepts from different academic traditions to explain the data.

Recent Rail Disasters, including Lac-Mégantic

There have been rail disasters in Canada in recent months, notably the event in Lac-Mégantic, Quebec in July 2013. Most of our interviews occurred before this event although some occurred after it. There has been considerable media coverage of Lac-Mégantic as well as other recent rail and pipeline events. As we point out in our report, media coverage is subject to several biases, which make us hesitant to draw conclusions at this point about any of these events; we await more information from official sources. We are interested to learn more about these events, and will be doing so in the coming months. For the purposes of this report, we do not focus

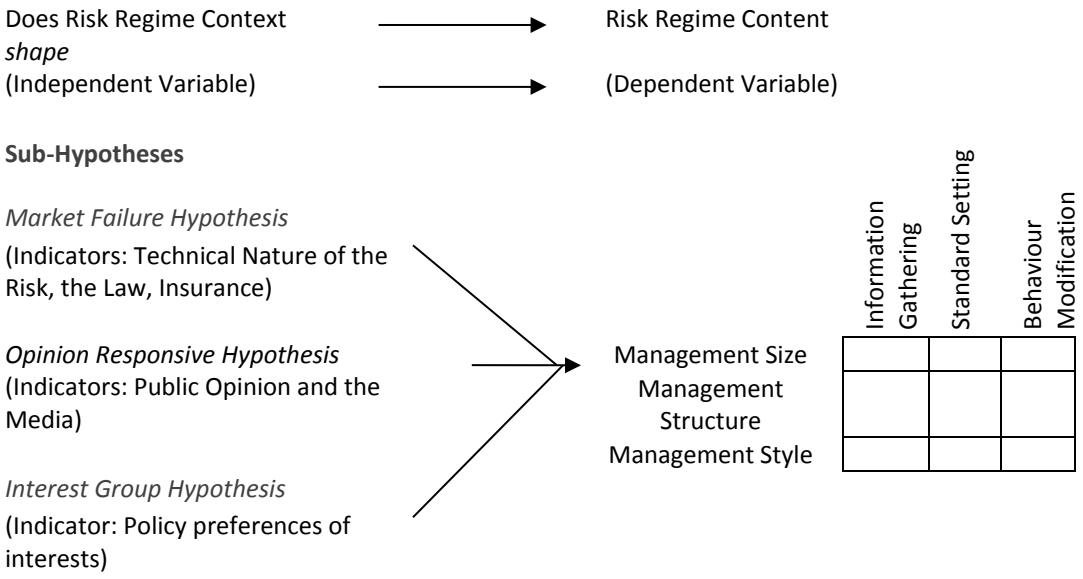
exclusively on these recent events. We do feel, however, that many of the observations we make about safety and security in the rail sector point to potential vulnerabilities in the subsector that pre-date these events.

3.0 The Framework

In their analysis of risk regulation regimes in the UK, Hood, Rothstein and Baldwin define regimes as "the complex of institutional geography, rules, practice and animating ideas that are associated with the regulation of a particular risk or hazard" (Hood *et al.*, 2001: 9). Hood *et al.* hypothesize that within these regimes context shapes the manner in which risk is regulated. 'Regime context' refers to the backdrop of regulation. There are three elements that Hood *et al.* use to explore context: the technical nature of the risk; the public's and media's opinions about the risk; and the way power and influence are concentrated in organized groups in the regime.

Hood *et al.* (2001) employ the cybernetic theory of control to examine the management of the specific policy area; they refer to this as 'regime content'. The theory asserts that if the three dimensions of control—information gathering, standard setting and behaviour modification—are under control, the system is effectively under control.

Figure 1: Hood, Rothstein and Baldwin (2001): Understanding Risk Regulation Regimes



We will discuss each of the three control components in turn. Information gathering is the capacity to obtain data that can be used to shape regime content. Information may be gathered actively or passively, both beyond the system and within it (Hood *et al.*, 2001: 22). Standard setting involves establishing goals, or guidelines; in government, standards often take the form of policy. Finally, behaviour modification refers to the preferences, incentive structures, beliefs and attitudes that shape systems—the capacity to modify behaviour of participants is the capacity to change systems. The distinction between these dimensions is not always tidy; Hood *et al.* (2001: 21) note, for instance, that information gathering may influence behaviour if people know they are being watched.

Each dimension of control may be further considered according to: size—the amount and scope of regulation and the resources used to sustain it; structure—the institutional arrangements of regime content, such as public-private sector relationships; and style—the formal and informal codes and conventions that help shape regime content (Hood *et al.*, 2001: 30-32).

3.1 Applying the Framework: Content

This section applies the Hood *et al.* framework to risks associated with the critical infrastructure of the Canadian transportation sector. The analysis relies on both the professional and academic literature and interview results to characterize the content of the risk regulatory regime for each of the transportation subsectors that we have selected: airports, seaports, trucking, rail and bridges.

3.1.1 Airports: Overview of Information Gathering, Standard Setting and Behaviour Modification

The information-gathering component of the airport regulatory regime is at times strong though not consistent across the sector. It is in part dependent on the capacity of an airport which, in general, is a corollary of size. (Interview 15 and Interview 13; hereafter 'interviews' will be referred to as 'Int' and followed by a number. Please see Appendix II for complete list of interviews.) Class 1 airports tend to have an extensive security and intelligence apparatus consisting of independent capacities and strong relations with law enforcement, security organizations and government (Int 1; Int 12; Int 13), whereas Class 2 and 3 airports tend to have less capacity; Class 3 in particular rely heavily on general government bulletins (Int 15). For example, certain class 1 airports have RCMP detachments located within the airport (Macdonald, 2014). In sum, information sharing between governments and the Class 1 airports is more complex and involved but also better integrated than at other airports (Int 12; Int 13; Int 15).

The mechanics of information gathering for government include inspections or compliance audits, the safety management system (SMS) and a variety of multi-organizational fora and advisory committees consisting of a multitude of government and industry stakeholders. Transport Canada is the lead government department (Transport Canada, 2013b) though other federal departments and agencies share responsibility for security, including the Canadian Air Transport Security Authority (CATSA) which is responsible for airline passenger and baggage screening. Information gathering occurs both formally (through these institutional mechanisms) and informally by virtue of the close working relationships developed, particularly by the large and better integrated airports (Int 12; Int 13; Int 15; Int 22). Airport operators are very confident that they know who to contact and that they would receive timely information from government concerning safety and security threats to their organizations. They also feel that airports have made considerable progress in recent years in assessing their threats, risks and vulnerabilities and in sharing that information with government (Int 12; Int 13; Int 15).

Unlike seaports, airports are not regulated with their own act. The industry was ostensibly economically deregulated in 1988 (Madore and Shaw, 1993). Airports within the National Airports System are not-for-profit, non-share capital corporations (Brooks and Prentice, 2001). These airports operate commercially and are locally managed and operated by Canadian Airport Authorities (CAA). The land and buildings are owned by the Government of Canada and the leasehold improvements revert to the Crown at the end of the management lease. Each CAA has a management lease and most are for 60 years with a clause for renewal for a shorter period. The industry, including the airports, is responsible for complying with and paying to meet government regulations (Transport Canada, 2011a).

Transport Canada's Aviation Security Oversight Program monitors and enforces stakeholder compliance and behaviour modification regulations through inspection activities and enforcement practices such as applying fines, or revoking operating licenses or certificates (Transport Canada, 20123b). One interview participant noted that Transport Canada is very active in its oversight of airports (Int 15). According to Transport Canada (2013b), the government takes a risk-based approach to airport security, meaning higher-probability and/or -consequence events receive more resources and attention. This approach includes an array of oversight activities such as focused security inspection and testing activities that are based on risk assessments, compliance results and threat information. The stated objective of Transport Canada (2013b) is to work collaboratively with airports and attempt to rectify any compliance issues with the least punitive measures possible. Transport Canada also ensures that the aviation security regime complies with Canada's obligations under international treaties (Transport Canada, 2013a).

Interview subjects have mixed feelings about Transport Canada's standards and enforcement. They feel generally that Transport Canada is engaged with industry and responsive to its concerns (Int 6; Int 7; Int 11). At the same time, the standard-setting component of the regulatory regime for airports is at times too standardized, according to interview subjects (Int 12; Int14). The legislation and regulations governing the aviation sector are extensive; indeed, aviation is considered to be one of the most aggressively regulated industries in Canada (Davis, 2001). Interview subjects stress that government should recognize the diversity in airports when applying the Canadian Aviation Regulations (2012), particularly issues such as size and use of facilities (Int 12; Int 13; Int 15). The cost of regulatory compliance is one of the most significant issues for some airports (Int 13).

Laws and legal concerns clearly weigh on the minds of airport operators, managers and regulators. Airports for the most part have business continuity plans and contingency plans in place and, in contrast to other subsectors, at times formal agreements with emergency services. When given a list of contextual issues relevant to our framework and asked which contextual issues influence the manner in which they spend their time with respect to safety and security, interview subjects in the aviation sector score law or legal concerns higher than any other contextual issue, and score it higher than did the other subsectors (ports or surface): 9.3 out of a

possible 10. (See Figure 2.) When asked, interview subjects expressed the most concern over risks associated with terrorism.

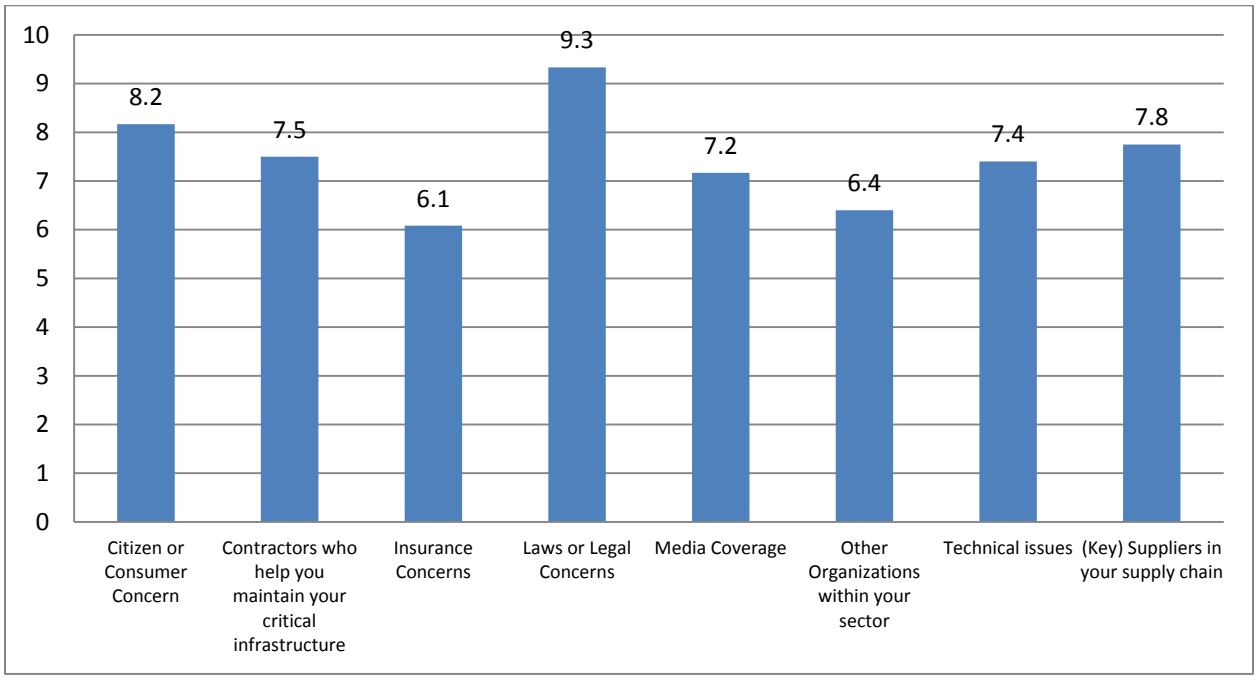


Figure 2: Responses from aviation interview participants to the question: "How would you rate the influence of the following subjects on how you spend your time with respect to matters of safety and security?" (n=6; results based on the mean rating given for each statement across participants on a 10-point scale in which 10 means 'very influential' or 'very demanding' and 1 means 'not at all' or 'I spend little time thinking about it')

Note about Figure 2: The small sample size in Figure 2 would preclude the use of any rigorous statistical analysis to support generalizations of the findings. We present the data as indicative of the relative importance of the contextual influences as assessed by these individual interview subjects and use it as a departure point for analysis and discussion. Please see the Methods section for further discussion on this approach.

In sum, information gathering for airports is largely cooperative and collaborative. There are clear, albeit extensive standards for security, which are developed largely by Transport Canada in consultation with industry and other stakeholders. Some interview subjects note that the regime is at times too inflexible and does not take the unique characteristics of each airport into account. Legal and policy concerns have considerable influence on airport staff. Transport Canada is active in behaviour modification, resulting in a robust, albeit at times routine- and rules-driven, control mechanism for the sector.

3.1.2 Seaports: Overview of Information-Gathering, Standard Setting and Behaviour Modification

The Canadian seaport system currently comprises 19 Canada Port Authorities (CPAs) that were created under the Canada Marine Act (1998). According to Brooks (2004), this is akin to a not-for-profit model. CPAs are "federally incorporated, autonomous, non-share corporations that operate at arm's-length from the federal government, which is the sole shareholder" (Transport Canada, 2013e). Three categories of ports exist in Canada: Canadian Port Authorities (CPA), regional/local ports and remote ports. Regional/local ports are those that are deemed to be in a position in which they could be better managed by local interests (Ircha, 2001.) Remote ports are those found in isolated communities that are reliant on marine transportation and have a government wharf (Brooks, 2007). In CPAs and remote ports, the government plays a strong regulatory role. Remote ports are considered to be a public good, and CPAs are considered to be essential infrastructure to the national ports system (Brooks, 2008).

As with airports, information gathering is stronger with larger ports than smaller ones. CPAs work closely with Transport Canada as well as the other security organizations. Information gathering is a combination of inspections and various fora that facilitate the exchange of information. The Interdepartmental Marine Security Working Group (IMSWG), for example, is a mechanism for information sharing between government agencies, and includes representatives of 17 federal departments and agencies (Transport Canada, 2013b). The interview subjects agree that the fora are useful for relationship building and networking (Int 32; Int 33; Int 41; Int 42). They allow port staff to engage with government officials (Int 33) as well as with local organizations and marine facilities that are not directly operated by the ports (Int 30).

At the same time, interview subjects are not entirely satisfied with information exchange about port security. They indicate that port staff need to spend much more time building relationships with stakeholders, including with other ports, emergency services, utilities and the various services that support port operations (Int 41; Int 42). They express concern that while they are prepared for regularly occurring threats, they are less well prepared for rare events (Int 41; Int 42). One participant notes that security information sharing is also very informal at times and depends perhaps too much on personal relationships within the law enforcement and security community, which can be *clannish* –a bit too inwardly accountable and only to those recognized as part of the identified community (Int 42; see Ouchi (1979) for reference to Clan control mechanisms). Trustworthiness between government and seaports seems to be constrained; Sloan (2012) notes there is evidence of organized crime and a lack of policing at seaports.

The regulations pertaining to risks within the marine sector are extensive. The primary legislation is the Marine Transportation Security Act (1994). The security framework created by these regulations includes inspections, monitoring, surveillance and enforcement. Security requires a large investment from both government and industry. The regulations are mandatory. While Transport Canada is the most significant public actor, several federal departments play a

role (Int 48; Int 42). As with airports, standards are significantly influenced by the international context. The International Maritime Organization's (IMO) International Ship and Port Facility Security (ISPS) Code to a degree standardizes and shares best practices.

Operators and managers at seaports find policy direction from government to be at times inadequate (Int 31; Int 32; Int 42). While there are security standards, interview subjects feel that there are no national standards for critical infrastructure and lines of responsibility for government departments and the policy direction themselves are unclear (Int 42; Int 32). Moreover, and in contrast to the aviation interviews, interview subjects feel that government security policies were not developed in a collaborative manner (Int 32). Government regulators are aware of these issues and acknowledge they sometimes face constraints when sharing information with external parties (Int 37; Int 38). As one participant notes, ports exist in an area of confusing multi-level governance (Int 48).

Many of the current standards for ports are perceived to be a government reaction to 9/11. While ship security has a long history, prior to 9/11 ports had not traditionally been as concerned with security. Some have described ports as starting from a clean slate after 9/11, and making considerable progress in a relatively short time. Interview subjects feel, however, that while some of these new standards are working well, others are not. As in aviation interviews, one participant recommends that government conduct a regulatory review examining these regulations to determine which of them should be kept and which should be discarded or redesigned (Int 31). Industry was particularly sensitive to the international context in which shipping occurs, including the international laws, competition, organized crime, terrorism and geo-political factors and felt that these pressures were not always sufficiently recognized by regulators (Int 35). There are also risks associated with passenger travel on cruise ships and ferries and inland shipping that some feel are not being adequately addressed.

This complex regulatory environment, combined with the occurrence of crime and competitive pressures ports face, creates a great deal of uncertainty and anxiety among staff (Int 29). This point was reinforced by the fact that when asked which contextual pressures influence the manner in which they spend their time, ports identify several and cannot clearly identify selected prevailing pressures. Of the eight potential pressures listed, participants score six between 7.0 and 7.8. This clustering of pressures is more pronounced in ports than in other subsectors. (See Figure 3.) When asked, interview subjects expressed the most concern over risks associated with climate change and extreme natural events.

Overall, port staff are much less satisfied than airport staff with the regulatory regime. While the federal government sets standards and audits compliance, interview subjects feel there has been insufficient effort to examine the sector as a whole and evaluate interdependencies, for example.

In sum, ports exist in an area of confusing multi-level governance; they are immovable, are expected to be competitive and serve a number of public and private sector interests. Compared

to airport interviewees, port subjects feel that information gathering is not as collaborative or cooperative and that standards and behaviour modification are driven by getting products to market as quickly as possible, which creates uncertainty and anxiety among port staff with respect to security.

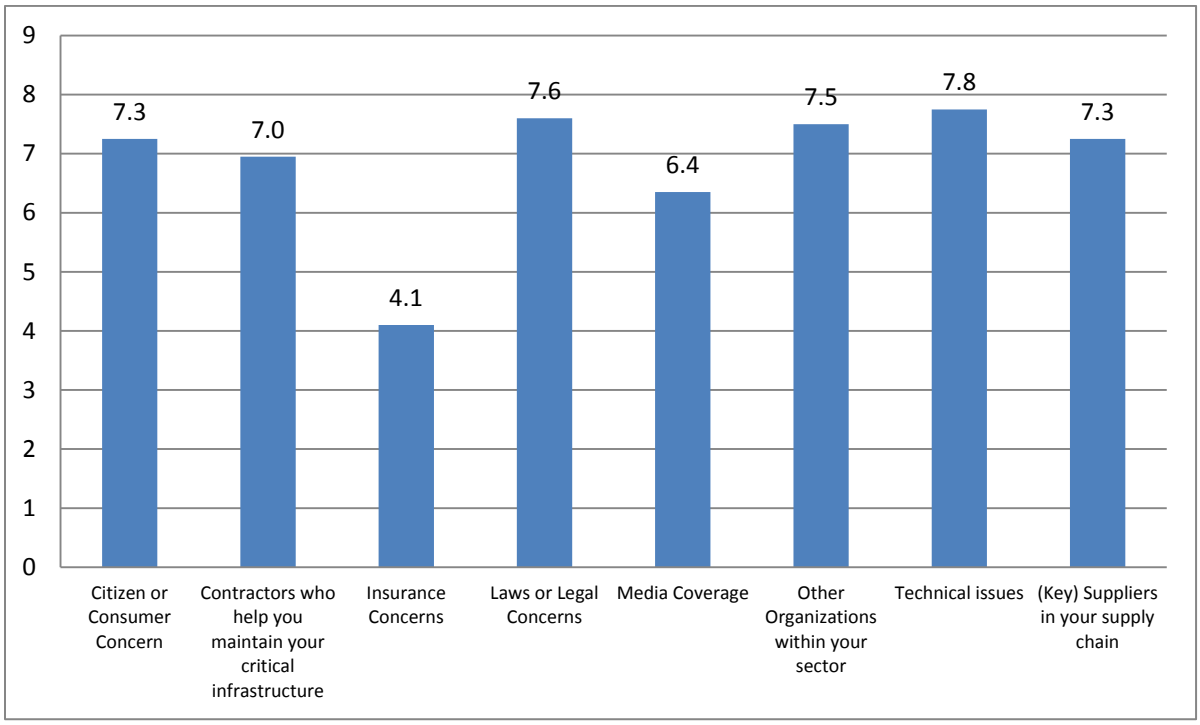


Figure 3: Responses from port interview participants to the question: "How would you rate the influence of the following subjects on how you spend your time with respect to matters of safety and security?" (n=9; results based on the mean rating given for each statement across participants on a 10-point scale in which 10 means 'very influential' or 'very demanding' and 1 means 'not at all' or 'I spend little time thinking about it'

Note about Figure 3: The small sample size in Figure 3 would preclude the use of any rigorous statistical analysis to support generalizations of the findings. We present the data as indicative of the relative importance of the contextual influences as assessed by these individual interview subjects and use it as a departure point for analysis and discussion. Please see the Methods section for further discussion on this approach.

3.1.3 Trucking and Rail: Overview of Information Gathering, Standard Setting and Behaviour Modification

Despite being quite different in many respects, trucking and rail are both categorized as "surface" and we therefore treat them together.

The trucking industry in Canada is made up of both corporations and small businesses. While some of these corporations are large, like TransForce with approximately 11,700 employees in

2012, by and large, the industry is constituted of smaller companies (CTA, 2012). This includes for-hire carriers, private carriers, owner-operators and courier firms, for a total of approximately 56,800 firms (Transport Canada, 2011b). From a security perspective, the information-gathering component is much less rigorous for trucking than for airport or seaports. Much of the information gathering regarding security comes from industry membership in voluntary organizations. Our interview findings suggest that the three programs described in Table 1 are among the most significant (Int 9; Int 10). Members voluntarily sign up for these programs because membership allows them to conduct their businesses more efficiently.

Table 1: Voluntary certification programs

Program	Description
Free and Secure Trade (FAST)	A voluntary government-industry joint initiative between the Canada Border Services Agency (CBSA) and U.S. Customs and Border Protection. Members are certified to a standard and then given access to faster border crossings (CBSA, 2013a)
Customs-Trade Partnership Against Terrorism (C-TPAT)	Similar to FAST—a voluntary government-industry joint initiative certifying industry to a standard that gives industries preferential treatment by U.S. Customs (C-TPAT, 2013)
Partners in Protection (PIP)	A voluntary CBSA program in which members agree to certain security standards. CBSA assesses industry on these measures, and also provides information sessions on security issues. Members are treated as lower risk by CBSA (CBSA, 2013b)

Trucking companies seem more willing than those in other subsectors to discuss, subject to very few conditions, safety and security at sector fora such as conferences or meetings (Int 9; Int 10). While information regarding vulnerabilities is not typically shared with anyone other than government, firms seem willing to discuss and compare procedures on issues such as access to buildings or other restricted areas. Interview subjects disagree on the extent to which the sector competes on safety and security issues (Int 9; Int 10). Interview subjects in trucking are more concerned about the theft of valuable freight than other types of risks. Indeed, cargo theft accounts for major losses in the transportation sector (Burges, 2012). Interview subjects noted the importance of collecting data in a consistent manner in order to appreciate fully the extent of the problem.

Rail contrasts significantly with trucking. While there are 31 federally regulated rail carriers in Canada (Office of the Auditor General of Canada, 2013), the rail industry is dominated by its three Class 1 carriers, Canadian National, Canadian Pacific (Int 45) and VIA Rail. As with other

subsectors, size and capacity are important themes in the rail interviews. CN and CP have their own police departments (Int 5). This allows the railways to be much more attuned to security issues and arguably more self-sufficient. Interview subjects feel information sharing between the railroads and their police forces is effective. In contrast, the smaller railroads and short lines rely significantly on the Railway Association of Canada (RAC); many also work closely with CN and CP for information-gathering (Int 45). Unlike airports, in which larger operations tend to be well integrated into government security information-sharing regimes, Class 1 carriers are less satisfied with information sharing with government. One interview subject from a Class 1 carrier stated that given the capacity of its own police force, much of the information shared with the rail sector by government is either redundant or dated (Int 5).

With respect to standards, trucking is much more fragmented from a regulatory perspective compared to airports or seaports (Brooks, 2008; Int 48). While there are some national standards, such as the National Safety Code (1987) and those issued by the Commercial Vehicle Safety Alliance, regulation is primarily a provincial responsibility and as a result the regime includes a variety of different regulations across the country (Kahai and Ford, 1997). Interprovincial trucking is nationally regulated but is still subject to the regulations of each province it enters. The voluntary certification programs listed above (FAST, C-TPAT and PIP) place obligations on firms to undertake a number of measures to improve their security procedures and adopt best practices, which entitles them to a lower risk classification. Gaining this status can expedite inspections and border crossings, and lead to fewer compliance audits. These programs apply not only to trucking but to rail as well.[2]

Inconsistency emerges as a recurring theme in the trucking interviews. Interview subjects cite the lack of uniformity in the credentials required for drivers to gain access to areas such as rail yards or ports as one example in a subsector with considerable inconsistencies across jurisdictions. Truck drivers undergo multiple checks, all verifying similar information to obtain access cards for the locations in which they deliver freight. One subject notes that this process has been streamlined in the U.S. (Int 9) although transportation specialists note execution problems there also.

Despite regulatory responsibility for rail being shared by the federal government and the provinces and territories, the influence of the federal government is more pronounced in rail and, as such, standards across the country are more uniform (Int 43; Int 44; Int 45). Unlike aviation or seaports, there is no act focused primarily on security for the rail sector: security is based on the Railway Safety Act (1985), the Transportation of Dangerous Goods Act (1985) and the International Bridges and Tunnels Act (2007). Recently, new provisions were added to the Railway Safety Act (1985) via the Safer Railways Act (2012), which aims at enhancing safety by creating a ‘culture of safety’ within railways and an industry-wide safety management system,

[2] C-TPAT and PIP also include manufacturers and retailers. PIP is the Canadian program and C-TPAT is the U.S. program; many Canadian and Mexican companies also belong to the U.S. program.

similar to the mechanism in place in aviation (Transport Canada, 2013g). There are no similar provisions concerning security.

While the recent audit by the Auditor General (2013) raised concerns about safety practices in rail, interview subjects underscore that in fact safety culture is much more pronounced in rail than security culture. One interview participant notes that there simply is not a culture of security present in the rail sector as there is with safety; security typically is not a priority and as a result is not considered in the majority of strategic planning sessions (Int 45). This is particularly true for short rail lines, which rely on the local community law enforcement and RAC for security concerns. As with trucking, standards for security are based on best practices shared between operators and derived from the economic incentive to remain a trusted participant in the overall system (Int 45). The security plans that railways do develop and submit to the regulators and industry associations tend to be high level and do not conform to any specific standard (Int 5).

When asked to describe the contextual issues that influence how they spend their time, rail reflect a more corporatist environment, which prizes stability; interview subjects are more concerned with the media and, like aviation, the law (see Figure 4). Trucking interview subjects, on the other hand, are more concerned with immediate market pressures, including insurance, the laws and citizens/consumers (see Figure 5). (Note that the number of interviews is lower in rail and trucking compared to the other subsectors; however, the interview subjects have strong industry-wide perspectives. We supplement this data with interviews with a number of public sector executives with responsibility for transportation as a whole.) When asked, trucking interview subjects expressed the most concern over risks associated with cargo theft and major collisions causing service disruption. When it comes to security, in particular, rail interview subjects expressed the most concern over risks associated with terrorism and public access points to rail infrastructure.

In sum, in trucking, information gathering seems less consistent, more dispersed and intermittent. Standards vary across jurisdictions, and behaviour modification depends on a number of market pressures in particular, including customer demand, insurance, laws and private rewards gained from membership in sometimes voluntary organizations. Individual service providers have less capacity to influence policy decisions; the sector as a whole seems ad hoc/less coherent in its approach to security than the other sectors. Whereas trucking seems to have a pluralist dynamic, rail has a corporatist one (Schmitter, 1977). Government and industry interactions are influenced significantly by CN and CP; laws and media attention influence their actions most. Economic and safety considerations receive attention; at the time of the interviews, security seems to be less of a concern. For SMEs, there is a reliance on the local law enforcement community and the RAC for information and standards regarding security risks.

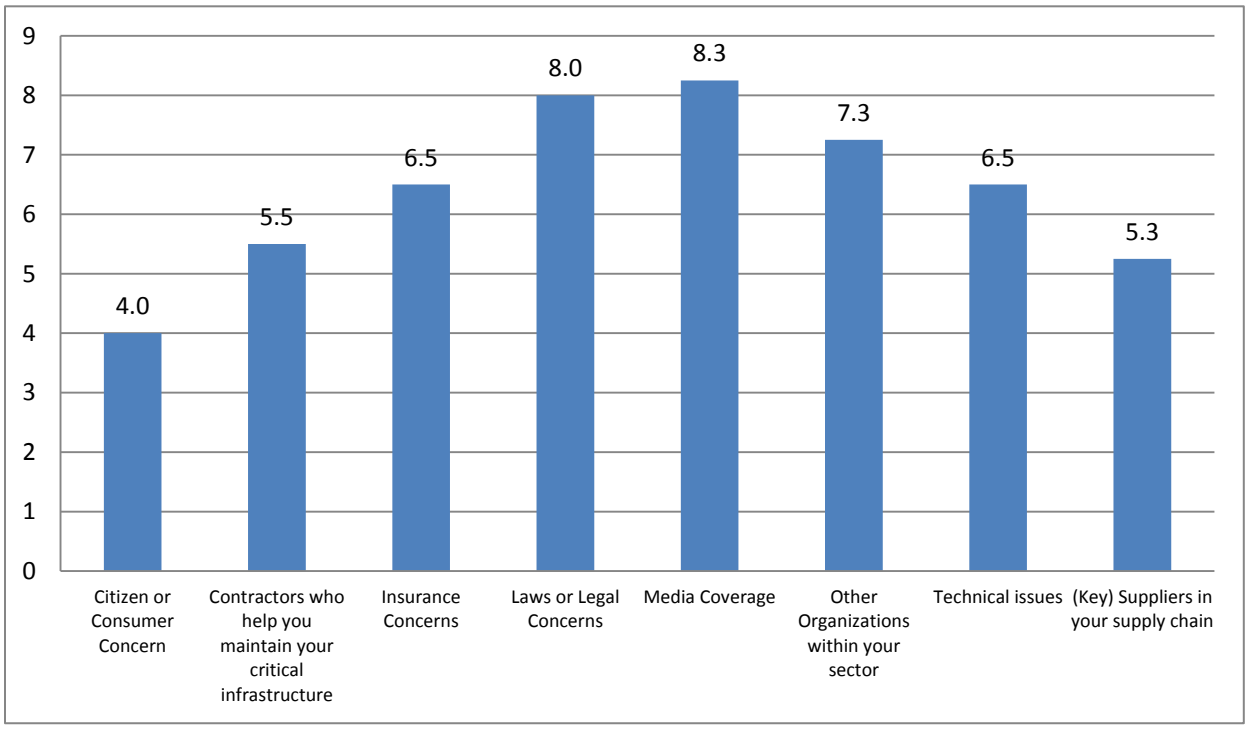


Figure 4: Responses from rail interview participants to the question: "How would you rate the influence of the following subjects on how you spend your time with respect to matters of safety and security?" (n=3; results based on the mean rating given for each statement across participants on a 10-point scale in which 10 means 'very influential' or 'very demanding' and 1 means 'not at all' or 'I spend little time thinking about it')

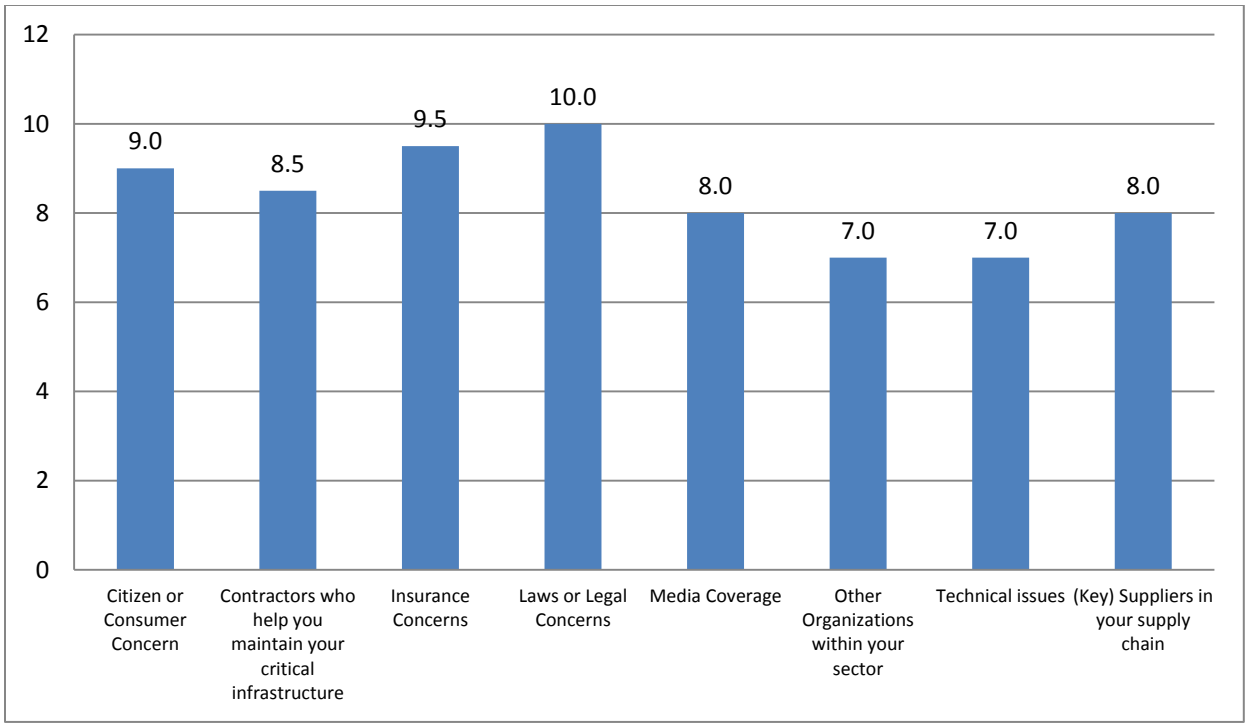


Figure 5: Responses from trucking interview participants to the question: "How would you rate the influence of the following subjects on how you spend your time with respect to matters of safety and security?" (n=2; results based on the mean rating given for each statement across participants on a 10-point scale in which 10 means 'very influential' or 'very demanding' and 1 means 'not at all' or 'I spend little time thinking about it')

Note about Figures 4 and 5: The small sample size would preclude the use of any rigorous statistical analysis to support generalizations of the findings. We present the data as indicative of the relative importance of the contextual influences as assessed by these individual interview subjects and use it as a departure point for analysis and discussion. Please see the Methods section for further discussion on this approach.

3.1.4 Bridges: Overview of Information Gathering, Standard Setting and Behaviour Modification

The principal formal mechanism through which government gathers information on bridges is through inspection. The nature and frequency of these inspections vary across provinces, but are predominantly designed to ensure compliance with safety standards. Security information is gathered and shared mainly through multi-organizational fora (Int 2; Int 16) and through strong informal relationships between bridge staff and government officials, and bridge staff with other bridges. Bridges, in general, almost uniquely so, are monopolistic and therefore do not engage in traditional market competition. This (arguably) facilitates strong information sharing between bridge owners, operators and managers, and government, both nationally and internationally (Int 2; Int 17). Some of our bridge interview participants are international; even some of those participants, far removed geographically, indicate a familiarity with the bridge community in

Canada and the presence of a strong network of information sharing informed predominantly by personal relationships (Int 2; Int 17).

Bridges are often under the jurisdiction of the provinces or local governments. Approximately 1% of the bridges in Canada are federally owned (Transport Canada, 2012b). Some are also privately owned; the federal railways, for example, maintain over 4,600 rail bridges across the country (Office of the Auditor General of Canada, 2013). Standards are primarily aimed at safety, with relatively less emphasis on security. The interviews do not refer to any concrete security standards for bridges in the Canadian or international context. The provincial safety standards vary; many include measures that relate to security, but are not expressly security standards. Bridges that fall under the federal International Bridges and Tunnels Act (2007) are the exception. This Act does include security measures, but they apply only to the 25 vehicular international bridges and tunnels, and nine international railway structures that are covered under the Act (Transport Canada, 2013f). Our interview participants, both Canadian and international, note that bridges tend to develop their own security measures in part by collaborating with other bridges and adapting standards used by them (Int 16, Int 18). These measures are shared best practices (Int 2) and not enforced by government oversight. For the majority of bridges, there are fewer clear security standards or protocols promulgated by government.

There are strong behaviour modification mechanisms in place with regards to safety; however, as already noted, there is an absence of clear standards for security and accordingly there is no formal mechanism to enforce security standards. One interview participant notes that security is mainly about communication with the security agencies; bridges are open and vulnerable and security is about sharing threat information (Int 16). When asked to weigh which contextual issues influence the manner in which they spend their day, bridge staff are more influenced by engineering risks and how the bridges are perceived by the media and public. Compared to the other sectors, they are less concerned about the law, insurance (most are self-insured) or about expanding their contacts with other owner and operators of critical infrastructure. (See Figure 6.) When asked, bridge staff expressed the most concern over risks associated with severe weather events.

In sum, major CI bridges are unique in the transportation sector in that they are effectively monopolistic. They are also immovable and open to the public and business, 24/7. They have limited built-in redundancy, or at least a failure has an immediate and significant impact in the broader community it serves. Bridge staff share information and best practices with staff from other bridges. They are mostly concerned with safety and technical/engineering risks. While there is a strong regulatory regime in place for safety, security is largely based on shared best practises and relationships with local law enforcement and other bridge staff.

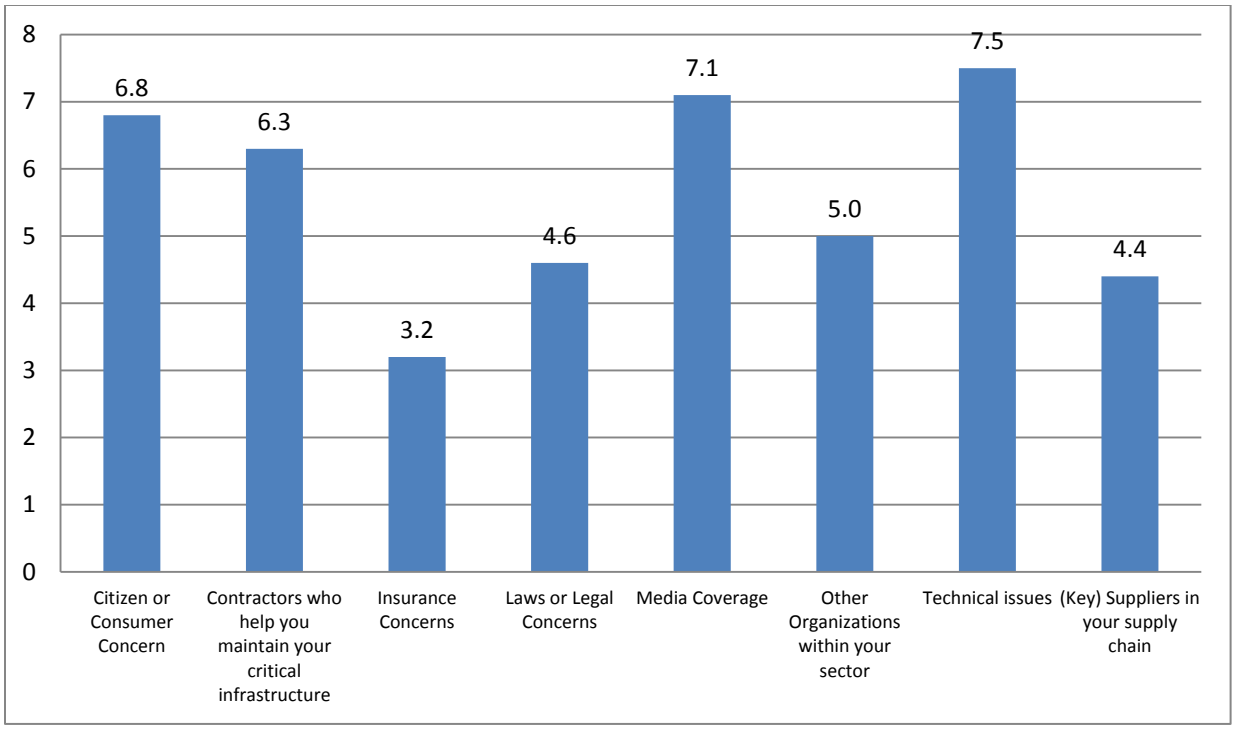


Figure 6: Responses from bridge interview participants to the question: "How would you rate the influence of the following subjects on how you spend your time with respect to matters of safety and security?" (n=5; results based on the mean rating given for each statement across participants on a 10-point scale in which 10 means 'very influential' or 'very demanding' and 1 means 'not at all' or 'I spend little time thinking about it.'

Note about Figure 6: The small sample size in Figure 6 would preclude the use of any rigorous statistical analysis to support generalizations of the findings. We present the data as indicative of the relative importance of the contextual influences as assessed by these individual interview subjects and use it as a departure point for analysis and discussion. Please see the Methods section for further discussion on this approach.

3.2: Interdependencies: All Subsectors

Interview subjects were shown a list of sectors identified by Public Safety Canada as critical and asked to identify three sectors upon which they rely the most in order to operate. Answers across subsectors were largely consistent: energy, telecommunications, emergency services, government and the transportation sector itself. Answers are noted in Figure 7.

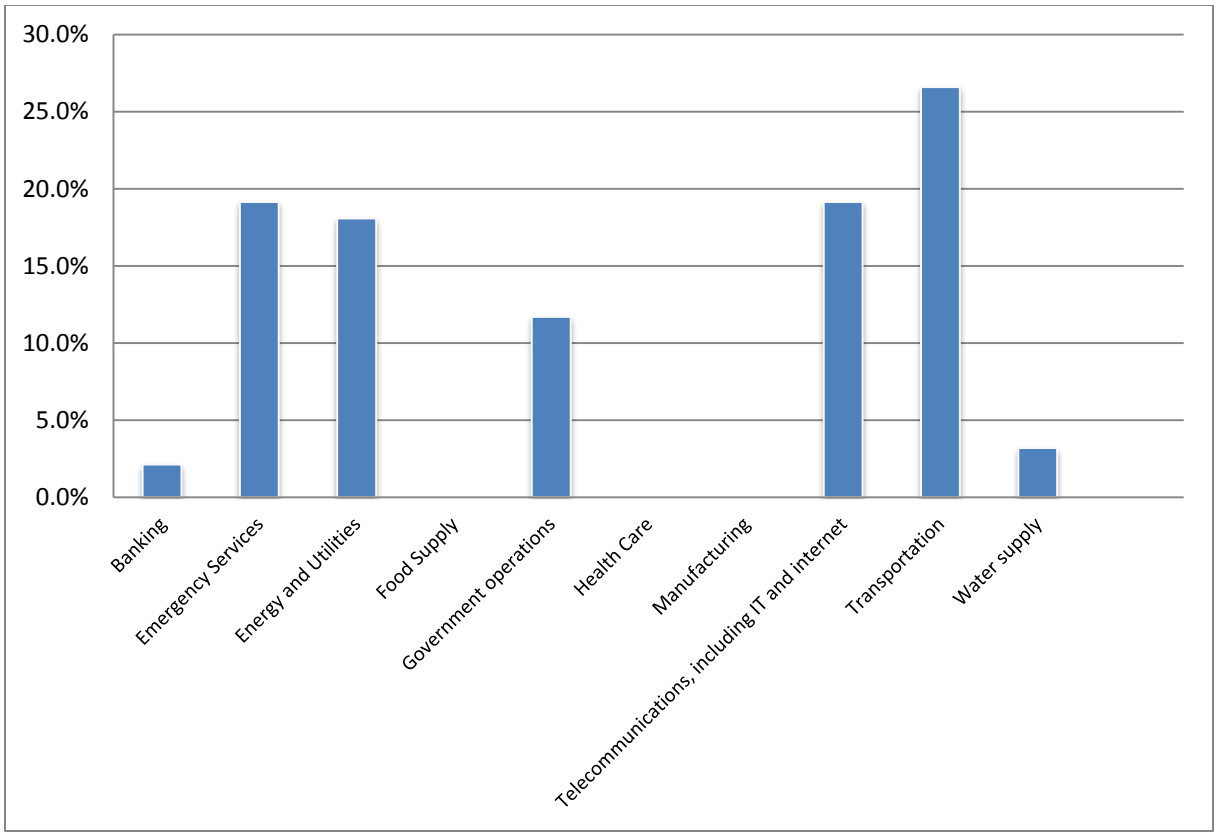


Figure 7: Responses from interview participants to the statement: "On which of these sectors do you rely the most to ensure successful operation of your business?"

(n = 33; results based on the percentage of participants that selected each response).

4.0 Risk Regulatory Regime: Context

4.1 Market Failure Hypothesis

Different types of ownership—from public to private—will dictate the degree of direct influence government has over the security of CI. The transportation sector is complex. The owner of the infrastructure is not common across the subsectors we studied. The largest seaports and airports are owned by the federal government but managed via a lease or concession, or corporatized commercial entity; smaller facilities may be owned by other orders of government or private companies. In trucking, ownership of the vehicles is widely fragmented while the largest share of the infrastructure used (both roads and bridges) is government-owned and -maintained, although there are some private roads and bridges. As for rail, the ownership is privately held by the railroads, while, in some cases, there are running rights held by public companies like VIA or private cargo owners.

While most sectors are regulated when it comes to safety and security, market structures vary considerably in the critical transportation infrastructure, which will impact the vulnerabilities to which the sector is exposed and the manner in which the subsectors will respond. Some subsectors are competitive (trucking) while others are monopolistic (bridges); some are heavily regulated (airports) while others have more flexibility (trucking); some are regulated primarily by one order of government (bridges, airports and seaports) while others are regulated by several (rail and trucking); some subsectors have considerable redundancies and are adaptive (trucking) while most have critical elements that are static/immovable and include high-consequence single-points of failure (seaports, airport, rail and bridges).

Security threats vary depending on the subsector, location and connection to international trade, and can range from those which capture the public's attention, such as terrorism, drug smuggling, people trafficking, people smuggling, to those which have perhaps more serious business implications, such as piracy, cargo theft and cyber-crimes, to the more mundane and probable, such as trespassing and petty crime. Many risks relate to broader questions of the underground economy in Canada, economic and political stability in parts of the developing world and access to key trade routes in international markets. There are also vulnerabilities to safety generated by communicable diseases, aging infrastructure and human error. The necessarily open and accessible nature in which public transportation operates also creates safety and security threats.

In order to understand better the challenges of CIP in the transportation subsectors, we will use two key measures that Hood *et al.* use to analyze risk regulation in markets: information costs and opt-out costs. Information costs are those incurred in assessing the level or type of risk exposure; opt-out costs are those incurred in withdrawing from risk exposure. In this section we examine the information costs and opt-out costs of the risks identified in our research. In so doing, we generate some estimates regarding the extent to which regime content, including

information gathering, standard setting and behaviour modification (IG, SS and BM), and the related size, structure and style, are functions of market failures. Figure 8 illustrates the concept by way of a two by two matrix.

		Cost of obtaining information on exposure to risk	
		Low	**High**
Costs of opting-out of exposure to risk by market or contractual means	**Low**	Minimal regulation	Regime content high on regulatory size for information gathering, with behaviour modification through information dissemination
	High	Regime content high on regulatory size for behaviour modification	Maximal regulation

Figure 8: Market failure explanation of regime size. Source: Hood et al. (2001: 74)

CI events can be catastrophic, and can devastate businesses and entire communities. When the survival of the firm is at stake, risk can no longer be described as the product of probability and expected monetary losses (Jaeger *et al*., 2001). In other words, when the firm is in danger of massive operational failure in the short term, conventional, long-term risk assessments do not necessarily hold. This short-term approach, however, would rarely describe how on an on-going basis an organization would approach risk.

Opting out of risk in the transportation sector depends largely on adaptive capacity and redundancies. The critical transportation infrastructure that we studied tends to be open to the public and, with the exception of trucking, fixed in its location. It cannot be easily moved, which creates opportunities for terrorists and criminals and challenges in the face of a rare natural disaster. Nevertheless, the transportation sector as a whole has a level of redundancy. Trucking, due to its atomistic nature and network structure, has greater adaptive capacity than the other subsectors; there are simply more routes to access in times of incidents and more service providers. Major CI sites, such as airports, seaports and bridges, can re-direct traffic to different outlets temporarily during CI events. Redundancy has cost implications, however, which, if not used, can seem to be a waste or unnecessary. Moreover, in a CI event in particular, the capacity of alternatives to accommodate requests might be limited given the immediate and increased demand for alternatives by numerous sources.

If adaptive capacity is important, then our interview subjects suggest there are vulnerabilities. Figure 9 shows how, on a scale of 1 to 10, four interview subjects scored their confidence in their business continuity plans following major threats to CI. Ten means ‘very confident’ and zero

means ‘no confidence at all.’ The results are not seen as widely variable, and they certainly do not inspire confidence.

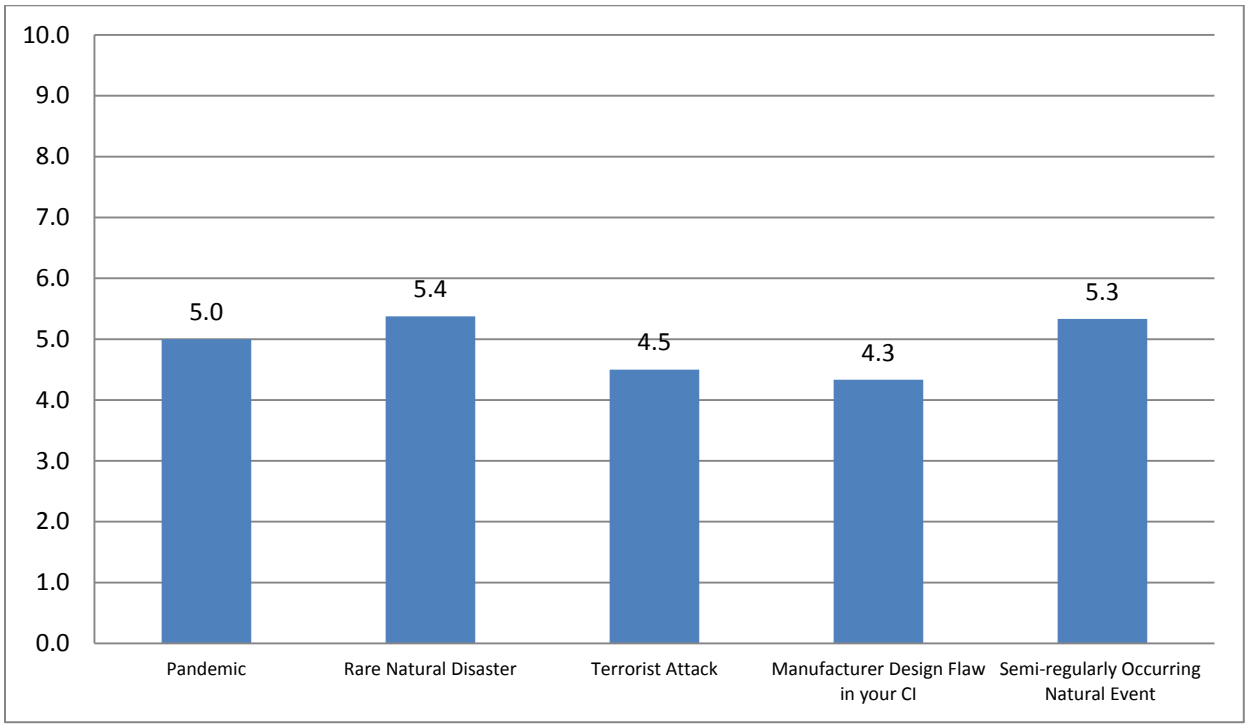


Figure 9: Responses from participants to the question: On a scale of one to ten, in which ten means ‘very confident’ and one means ‘not confident at all’, how confident are you in your business continuity plans following this event?’ N=4.

Note about Figure 9: The small sample size in Figure 9 would preclude the use of any rigorous statistical analysis to support generalizations of the findings. We present the data as indicative and use it as a departure point for analysis and discussion. Please see the Methods section for further discussion on this approach.

Typically, opting out of risks is difficult. Supply chains are complex, interdependent, growing and increasingly global. They are challenging to model, which makes it difficult for the market to develop reliable insurance policies. This is especially so for terrorism (Boardman, 2005), some criminal activity or rare natural disasters in which data is too scarce and unreliable. Adaptive adversaries, as we have in terrorism and criminal activity, make opting out even more challenging as adversaries (unlike natural disasters) react to the risk strategies agencies put in place. Managing low-probability risks in a robust manner can rarely be justified at the firm level (Seidenstat, 2004); security is usually seen as a negative expense. Market-sensitive organizations will often not take pronounced steps to protect against low-probability/high-consequence events (Jaeger *et al.*, 2001).

Despite in some cases being privately owned or at least privately operated, CI is crucial for our collective well-being and as a result governments are unlikely to let the service, if not the organizations which run them, fail outright, particularly monopolies and oligopolies. This arguably creates a moral hazard. After disasters and to varying degrees, governments often have to assume their role of insurer of last resort and assist in recovery efforts. Note in Figures 2-6 that only trucking subjects described insurance as something that influenced their behaviour. Many large CI organizations, in fact, are self-insured.

The rule of law is an important mechanism for opting out of risk exposure but has limitations. Shore (2008) argues that there is a legal imperative on the part of both government and private enterprise to protect CI from terrorist events, for instance. Essentially, government and industry need to take reasonable steps—risk assessments, business continuity plans, for example—to protect CI. The complexity and interdependence in CI, however, makes it very difficult to identify the parties who are responsible for the failures. Legal processes can also take time. The rule of law is even more limited at the international level. Collaboration between friendly Western nations can be difficult and time-consuming due to different legal contexts; collaboration with nations without stable governance—which is sometimes the case on or near critical international trade routes—poses even more substantial challenges.

There are some options. The U.S. government's treatment of BP after the 2010 oil spill in the Gulf of Mexico provides an interesting example of government applying pressure publicly on a company, such that it likely undermined the company's ability to conduct business and even raise private capital. This tactic does not preclude a legal process from occurring but arguably prompts a more immediate response from the company than a protracted legal process.

The difficulty in opting out of risk makes information exchange among owners, operators and managers even more important. Indeed, the primary CI initiatives in Canada and other Western countries put considerable emphasis on information sharing. (See, for example, Public Safety Canada, 2009; Australia's Attorney-General's Department, 2003; United Kingdom: Centre for the Protection of National Infrastructure, 2006; United States: Department of Homeland Security, 2008.) Yet information sharing is constrained by a number of issues, including complexity and uncertainty (Renn, 2008), legal barriers, capacity, institutional culture (Hood, 1998) and most notably for the market failure hypothesis, competition. While a firm may share information with suppliers to ensure that a supply chain functions efficiently and securely, and resilience can provide a potential competitive advantage (Sheffi, 2005), companies are unlikely to disclose sensitive information to competitors. Moreover, company vulnerabilities or outright failures tend to be "dirty little secrets;" industry leaders are reluctant to discuss the vulnerabilities of assets because of the risk to their organization's security, liability, share value and public image (Quigley, 2013).

The theme of constraints due to competition occurred more frequently in interviews with seaports, rail and trucking. Seaports and rail, in particular, showed less willingness or capability

to share information outside of their organizations. Despite being competitive, trucking showed more willingness to share information but was constrained by lack of capacity and incentive.

Competition, however, can be a red herring. Bridges do not compete, and airports do not compete on security, in particular (Int 13; Forsyth, 2007; Hancioglu, 2008). At first blush, it was not surprising to learn that these subsectors shared information more willingly with others within their respective sectors. Yet monopolies and oligopolies also have a number of reasons not to disclose information about vulnerabilities, and in fact, many are similar to the reasons of more competitive firms (brand, liability, security, for example). Arguably, monopolies and oligopolies have a greater capacity to control much of the information in their organization; ironically, a highly competitive pluralist context with many suppliers can actually make information more readily available to regulators. If these less competitive monopolies and oligopolies are more likely to share information, it can likely be attributed to the seriousness of CI failures, their sometimes more stable and collegial relationship with regulators and—for the purposes of this hypothesis—not wishing to be held liable.

There are opportunities to encourage information exchange about risks and vulnerabilities in a context in which information is not readily shared. Looking carefully at lessons identified from past experiences—both disasters and near misses, in Canada and abroad—provides learning opportunities, for example, that regulators should exploit in order to reduce information costs. Ensuring privacy and proprietary information rights are maintained and signing formal non-disclosure agreements can also help; so too can encouraging 'best practices' in business continuity from across the industry.

Returning to Figure 8, due to the high information costs and high opt-out costs, one might expect to see a strong regulatory stance by government—maximal regulation as depicted in the figure. At the same time, the market seems to be working; in fact, demand for transportation is growing and the sector has largely met this demand. In the more competitive subsectors, risk management plans must also consider opportunity costs. A robust regulatory stance without concrete evidence of problems may result in reduced competitiveness of these sectors. In other words, a narrow focus on low-probability events might reduce the probability marginally but generate a much higher cost in lost efficiencies. While a maximal regulatory stance at present may seem excessive, government's role of collecting and validating information against appropriate safety and security standards becomes important. It allows regulators and industry to track problems and determine if CI incidents and vulnerabilities are increasing. Reliable information-gathering can be an important early warning strategy that can help to address events before they occur.

In sum, economists argue that safety and security in the transportation sector constitute a market failure. The market would not provide them at a socially optimal level without government intervention (Hainmüller and Lemnitzer, 2003; Savage, 2001; Seidenstat, 2004). Opt-out costs are usually high in risks associated with the critical transportation infrastructure we studied (although trucking under certain circumstances may be an exception). Information costs can also

be high but vary according to the nature of the risk. Government CI initiatives focus extensively on information-sharing strategies, which are important but require an intimate knowledge of the subsector to be effective. Depending on the subsector and indeed the organization, competition, incentives, penalties, confidence, willingness, perceived importance of the information, concern over leaks, authority, organizational culture, market sensitivities, ownership and capacity, for example, can influence the extent to which organizations choose to share information. (This will be discussed further in the Interests section.)

It is difficult to justify the costs of managing low-probability events and as a result governments likely have a strong role to play in collecting and validating information and also in enforcing standards and behaviour change before events. The complexity and uncertainty of the risk (Renn, 2008) and lack of incentives on the industry side, particularly among SMEs, create a potential moral hazard; governments must ensure sufficient standards and behaviour modification practices are in place to ensure that owners, operators and managers take responsibility for their operations and are held accountable for failures. (Subsector-specific strategies are discussed in more detail in the Interests section.)

Hood *et al.* (2001: 71) argue that the market failure hypothesis (MFH) is "more useful as a method of analytical benchmarking than as a reliable predictor of regulatory content." While the MFH highlights the importance of implementing stronger controls across all three components of the cybernetic control spectrum (IG, SS and BM), such a move could be excessive, given the risk. At the same time, the hypothesis is not fully satisfying because it leaves open the possibility of low-probability failures, to which the public typically has a strong and arguably irrational aversion—a point we will look at in the next section.

4.2 Opinion-Responsive Hypothesis

Hood *et al.*'s (2001) opinion-responsive hypothesis seeks to examine the extent to which public preferences and attitudes influence the regulatory regime. Though there are limitations in attempting to measure public opinion, media coverage and polling data offer some insight. By examining the extent to which the regulatory content reflects these public opinions, we can make some assessments regarding the strength of this hypothesis. We first look at the psychology of risk to understand why people react in the manner they do to low-probability/high-consequence failures, which cannot be explained strictly in rational terms. Secondly, we look at the role of the media as an important social amplifier of risks to examine more closely how they depict low-probability/high-consequence events.

The Psychology of Risk

Probability and consequence are at the core of any risk calculation. This rationale for risk, however, depends on a rational actor paradigm (RAP) in which probability and consequence are objective and (reasonably) obtainable measures (Jaeger *et al.*, 2001). According to the

psychology literature, the psychometric paradigm, in contrast, conceptualizes risks as personal expressions of individual fears or expectations. Individuals respond to their perceptions whether or not these perceptions reflect reality. The psychometric approach seeks to explain why individuals do not base their risk judgments on expected values, as RAP advocates would suggest (Jaeger *et al.*, 2001: 102-104). The approach has identified several biases in people's ability to draw inferences. Risk perception can be influenced by properties such as perception of dread (Slovic *et al.*, 1982), personal control (Langer, 1975), familiarity (Tversky and Kahneman, 1973), exit options (Starr, 1969), equitable sharing of both benefits and risks (Finucane *et al.*, 2000) and the potential to blame an institution or person (Douglas and Wildavsky, 1982). It can also be associated with how a person feels about something, such as a particular technology or a disease (Alhakami and Slovic, 1994). People also show confirmation bias (Wason, 1960), which denotes people's tendency to seek out information to reinforce pre-existing beliefs. People can also be vulnerable to 'probability neglect' (Slovic *et al.*, 2004). When probability neglect is at work, "people's attention is focused on the bad outcome itself, and they are inattentive to the fact that it is unlikely to occur" (Sunstein, 2003: 122). Indeed, psychologists have noted that the reporting of one death, particularly that of a child, if framed in a certain manner can prompt strong emotional reactions and extensive media coverage (Slovic, 2011; Kearney, 2013).

Sandman *et al.* (2012) propose a model to explain public perception of risk as a function of two components, hazard and outrage. The former refers to the technical expert risk assessment of the event while the latter refers to the emotional reaction people have concerning the event. The authors list 20 characteristics of events that affect the magnitude of outrage, many of which can be identified in catastrophic events. Figure 10 shows the volatility of public opinion on an issue like terrorism.

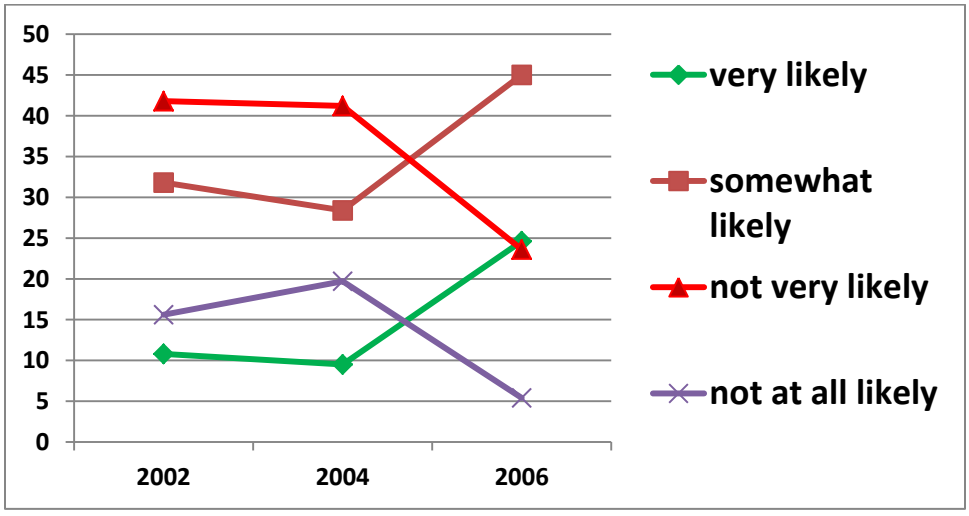


Figure 10: Three public opinion polls: Do you think it is … that Canada will be the victim of a major terrorist attack in the next two years? (Environics Institute, 2002, 2004, 2006)

Media Coverage

There is a well-established literature on the agenda-setting function of media (Mutz and Soss, 1997; McCombs, 2005; Cobb and Primo, 2003). Media coverage has significant impact on the salience of the topic on the public agenda. As Cohen (1983) famously observed, however, media coverage is very influential in telling the public what to think about, but less so in telling the public what to think. A psychometric approach to risk provides more insight into the effect of media than a rational one. Researchers have noted the media's propensity to report the dramatic over the common but more dangerous (Soumerai *et al.*, 1992) and their tendency not only to sensationalize (Johnson and Covello, 1987), but to sensationalize the most negative aspects of events (Wahlberg and Sjoberg, 2000).

Many of these emotionally charged and amplified events in which media and social commentators rush to impose meaning will ultimately lead to a selective search for blame and accountability. Pidgeon (1997: 9) argues that "despite the inherent complexity and ambiguity of the environments within which large-scale hazards arise, and the systemic nature of breakdowns in safety, cultural myths of control over affairs ensure that a culprit must be found after a disaster or crisis has unfolded."

Figure 11 is the result of an analysis of media coverage of selected CI events that have occurred post-9/11. The analysis examines articles that appeared over a 365-day period in one national newspaper from the country in which the event occurred. Figure 11 shows volume of media coverage on the Y-axis and the manner in which the media assessed government performance on the X-axis. Countries include Australia, Canada, the UK and the U.S. Events include natural disasters, industrial (including chemical) failures, food contamination and failed terrorist plots. (For a more complete discussion of the media analysis, please see the Methods section.)

The transportation-specific events include the I-35W Bridge Collapse in Minneapolis, the Waterfall Train Accident in Australia, De la Concorde Bridge Collapse in Montreal and the Potters Bar Train Wreck in the UK. A complete list of events is found in Appendix III.

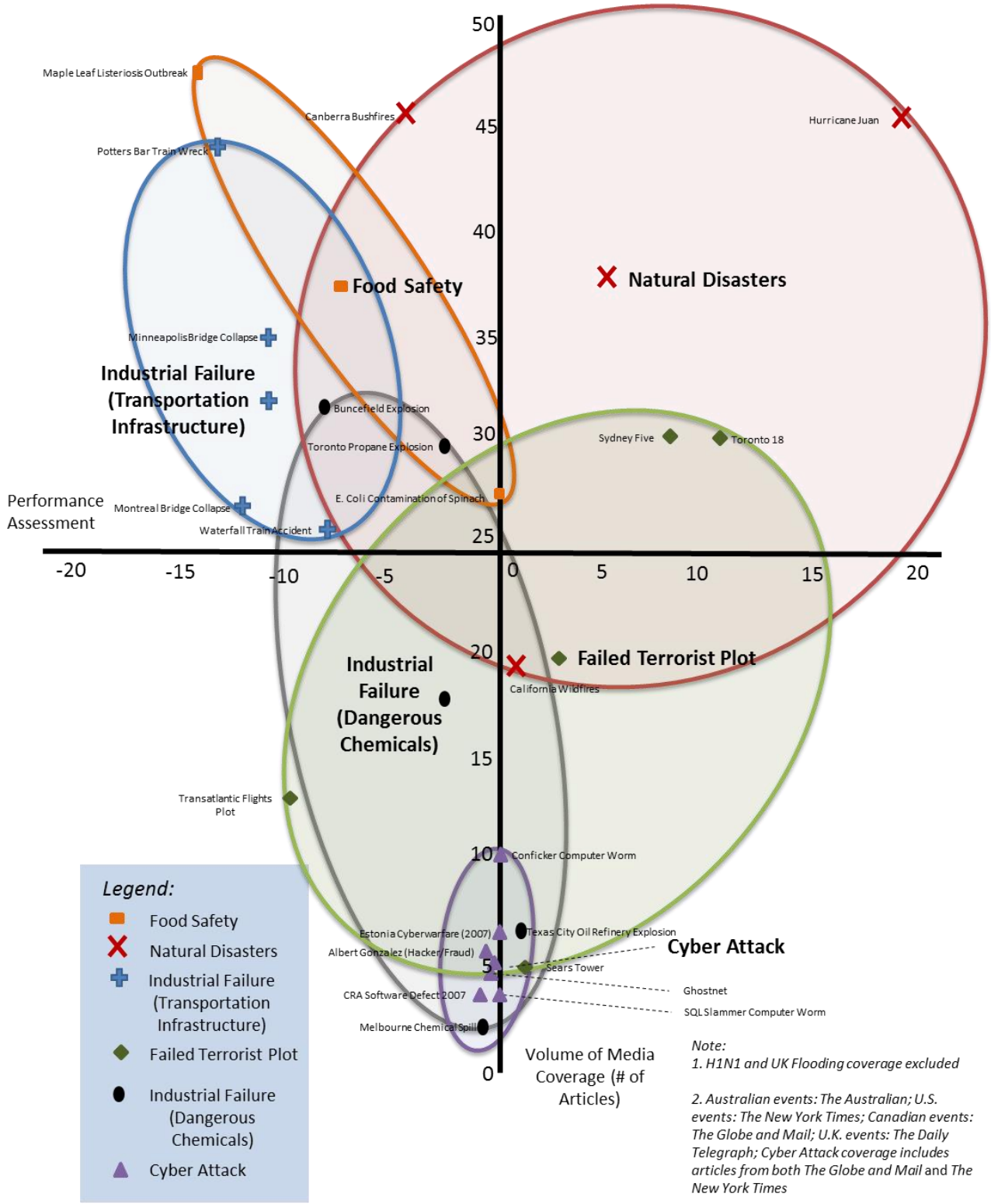


Figure 11: All hazards: Government performance assessment and volume of coverage in print media by event type (Australia, Canada, UK, U.S.)

We realize the number of events is relatively low and therefore we have to be careful about the conclusions we draw. Nevertheless, some patterns emerge and they are reinforced by other academic research. The transportation events in Figure 11 are the result of industrial failures and not malicious intent. They received a comparatively high volume of coverage and included, on balance, many more negative assessments of government performance than positive ones. As Pidgeon (1997) notes, industrial failures typically include a somewhat ruthless hunt for accountability. Coverage following natural disasters, on the other hand, tends to be high volume but much more forgiving, as we see in Figure 11. This is particularly ironic because natural disasters actually kill and cost more than industrial failures (Caruson and MacManus, 2011) and as Steinberg (2000) notes, many policy decisions are taken well in advance of natural disasters that help or hinder our capacity to respond to them. For failed terrorist plots, we selected cases that have been framed in the popular media and discourse as having been perpetrated by radical Islamic fundamentalists, inspired by Al-Qaeda. Our analysis of these events shows moderately high levels of coverage and depicts governments positively, particularly in *The Globe and Mail* and *The Australian* (Quigley *et al.*, 2013). Arguably, the Australian and Canadian cases had an element of novelty; up until the point of the arrests, neither country had experienced such a domestic event framed as radical Islamic fundamentalist terrorist attack post 9/11.

Typically, cyber plots receive very little coverage; they receive more coverage if they can identify a culpable party, which is not always easy in cyber stories. While not included in Figure 11, media coverage can also be higher when victims of cyber-crime are part of a vulnerable group, as with child pornography or cyber-bullying. We have also seen a rise recently in stories concerning spying, insider threats and the collection of *meta* data. These are relatively recent stories and our research to-date has not examined this media coverage in detail. It would seem that the ability to identify an individual as being primarily responsible (e.g., Edward Snowden, Julian Assange and Chelsea Manning) has helped to generate more coverage.

Another pattern to this media coverage is that it spikes and then falls away. Of the events we looked at, about 70% of total coverage occurred in the first month after the event. There can be a second peak in the coverage depending on whether or not there is an investigation, an inquiry, an audit, a commission or a trial. This second peak can occur anywhere from six months (inquiries) to two or three years (trials) after the event. It is usually much smaller and shorter-lived than the first peak in coverage. Understanding exactly who is responsible for the event can also take some time. Industrial failures are typically very complex. This delay between spikes represents a gap between the event itself and the identification of culpable parties or at least the provision of an explanation, which arguably lessens the impact of the (quasi-)judicial process and appropriate sense of accountability in the public's eye.

Regulatory regimes do not necessarily reflect the scale of the hazard but rather the profile of the hazard. In industries where hazards and risks are visible and of public interest, there is less resistance to implementing regulations (Lindøe *et al.*, 2011). These industries can also represent preferred targets for terrorists (Jenkins, 1998). Despite the fact that commercial flights remain

the safest way to travel, plane crashes receive a disproportionately high volume of media coverage (Cobb and Primo, 2003). The high level of regulation in the aviation sector may be partially explained by the high dread and low control factors (Slovic *et al*., 2004) and the availability heuristic triggered by such events as 9/11 (Kahneman and Tversky, 1982). This likely explains the focus on airport security, as an extension of aviation security because airports are the primary access point for airplanes. In order to have public confidence in the system, government regulates extensively and industry cooperates as it is clearly in their interest to do so. It is also true that aviation has a tradition of stringent security practices; in many respects, post-9/11 practices simply built on this tradition.

Other subsectors do not receive the same level of attention as airports. Rail, as witnessed in the Madrid bombing, the London Underground Bombing, the Moscow Subway bombing and the 2013 arrests in Canada over an alleged plot to attack VIA Rail, can also be a target for terrorists, but we have yet to see the kinds of security checks in trains and subways as we see in airports. Unlike airports, however, increased security in rail would require a significant change in approach to security than has traditionally occurred, which would increase costs and inconvenience.

Further attacks in these other subsectors could reframe the issue for the public, especially if they have a stronger emotional impact on the public. Should pirates (or terrorists) capture a public ferry or cruise ship in Canadian waters, for example, the risk psychology literature would suggest that the media coverage and public and political attention concerning piracy would almost certainly be higher volume, more alarming and immediate than it is now.

The Opinion-Responsive Hypothesis also raises the question about whether (and if so, the extent to which) people wish to live in a state in which security practices are so obvious. In the case of airports, enhanced security adds not just cost and inconvenience but security theatre (Schneier, 2003; Stewart and Mueller, 2011), which can be reassuring but also unnerving. By this measure, seaports and rail stations arguably generate different controversies. Unlike airports, seaports and rail stations are often built into the historic landscape, particularly so for older cities. Putting a fence and CCTV cameras around a modern and remote or suburban station or seaport may not spark the same controversy as putting a fence around centrally located transportation facilities in the downtown core of a historic city.

The Opinion-Responsive Hypothesis prompts observations about transportation's risk regulatory regime in the immediate aftermath of security events, in particular. First, government's emphasis on information sharing is likely to be inadequate in the event of disaster, according to this hypothesis. In the short term, media coverage and public opinion will likely look for higher standards backed by stronger methods of behaviour modification. How blame will be apportioned will partly be a function of how the issue is framed; most parties (regulators and industry), however, are depicted as having performed poorly following industrial failures. Secondly, the Opinion-Responsive Hypothesis raises the question of *who* should be directing the

regulation regime in the case of a security event. When we discuss CI protection, we emphasize information sharing and collaboration. However, in the event of a crisis that is perceived to impact national security, people will likely want their own governments to play the lead role. In the event of an industrial failure, however, an arms-length, third party auditor would likely have more credibility with respect to the assessment.

Finally, the Opinion-Responsive Hypothesis suggests that after a disaster, and for a short period of time, media and public opinion (however volatile) come into play with greater force. Arguably, this disrupts the normal control mechanism and creates opportunities for change, which under normal circumstances are subject to (at a minimum) path dependency and organizational inertia, if not resisted outright by many of the dominant interests. This change in dynamic can present opportunities to overcome entrenched interests and inertia but also creates problems with over-reactions. Focussing on highly emotive issues (and neglecting more probable and consequential risks) can attract attention and for a limited period motivate change to the regulatory regime but can also lead to narrow and misguided risk assessments. Our data suggests, for example, that media coverage of extreme natural events seems less likely to lead to dramatic changes than industrial failures would. Recall that interview subjects from seaports and bridges noted that extreme natural events are the risks that concerned them the most. In contrast, media coverage of industrial failures is susceptible to blaming individuals, or looking for a "bad guy" to blame. This approach over-looks the more systemic issues that may underpin the true vulnerabilities in industrial failures. More complete information in the public domain that addresses knowledge gaps can help to mature the public's (and the media's) opinions on security issues, and in so doing offset the likelihood and consequences of over- (and sometimes misdirected) reaction.

In sum, public opinion can be volatile; the psychology of risk literature provides insight into the somewhat irrational reaction people have to risk. Low-probability/high-consequence events generate high-volume media coverage for a short time. Different types of events—natural disasters, industrial failures, terrorist plots, criminal activity, cyber events—generate different types of coverage, not just in volume but in tone and in their search for accountability. (For a more comprehensive analysis see Quigley *et al*., 2012, 2013). Industrial failures in the transportation sector seem to generate particularly negative, alarming and high-volume media coverage. Focussing on highly emotive issues can motivate change for a limited time but can also lead to misguided risk assessments. More complete information in the public domain can help to fill knowledge gaps and offset the likelihood and consequences of over-reaction.

4.3 Interest Group Hypothesis

Cultural Theory

In this section we explore the different pressures and expectations that organized interests have on the regulatory regime. Hood *et al*. (2001) note that interest group pressures are often a more reliable predictor of content than the other two hypotheses.

CI includes a variety of organizational types, including monopolies, oligopolies and competitive markets. While most sectors are regulated when it comes to safety and security, the degree, complexity, style and process vary. In their study of risk, Hood *et al.* (2001) used Wilson's (1980) typology to analyse interests. Given the data we have available, we have opted for a Cultural Theory analysis. Cultural Theory (Douglas, 1982, 1992; Hood, 1998) can be useful in interpreting how different organizational types respond to risk. Cultural theorists see risk not as a calculable probability, but rather as a danger or threat to a value system, which is embedded in the institutional arrangements. Anthropologist and cultural theorist Mary Douglas notes, "Certainty is only possible because doubt is blocked institutionally. Most individual decisions about risk are taken under pressure from institutions" (Douglas, 2001, xix). Hood (1998) used the theory to explore the recurring nature of debates about public administration and the irreconcilable assumptions underpinning different views and preferences. The theory measures regulation and social integration to determine value systems and the preferred institutional arrangements flowing from them, leading to the characterization of four types: hierarchists, individualists, egalitarians and fatalists (see Figure 12). Each type has a preferred governance arrangement, particular blind spots and vulnerabilities.

Cultural Theory has had limited success when tested empirically (see, for example, Dake, 1991; Sjöberg, 1998). Dake had some success but notes that at the level of an individual the correlations between culture and bias are weak and of limited predictive value. The regulation/integration typology is also criticized on the grounds that the categories in the typology are too limiting. Assumptions about risk perception are far more complex and dynamic than the categories imply (Renn *et al.*, 1992) and Cultural Theory also fails to take the media into account (Zinn, 2004: 15). At the same time, its capacity to show the recurring debates and irreconcilable difference in these debates has been described as a revolutionary advance in the study of risk (Royal Society, 1992) and Hood's (1998) use of the theory to explore the recurring debates in public administration is a particularly recognized study.[3]

Like Hood, we use Cultural Theory here as a heuristic device in order to structure an analysis of (in our case) the transportation sector. It can be applied at the macro, meso and micro levels. No

[3] Hood's *The Art of the State: Culture, Rhetoric, and Public Management* won the UK Political Studies Association's W.J.M. Mackenzie book prize in 2000 for the best book published the previous year in political science.

subsector will fulfill all the requirements of any one of the four types. Rather, organizations show tendencies, and these tendencies can be particularly strong in the aftermath of a failure; this can be helpful in anticipating who or what the organization blames when things go wrong and the pressures and demands each sector is likely to make on the regulatory regime. The analysis is conducted in comparative perspective across the subsectors in transportation that we analyze. When we note, for instance, that trucking best meets the criteria of the individualist, this means that trucking seems to have more individualist tendencies than the other subsectors in transportation.

We make two final notes about Cultural Theory. First, most organizations will see aspects of themselves in all four types. Many, in fact, move towards the centre of the regulation/integration typology. A bureaucracy (hierarchical), for example, is still sensitive to competition (individualist), values 'round tables' (egalitarian) and recognizes the chaos that ensues when an unpredictable event occurs (fatalists). Cultural Theory suggests that organizations will tend towards one type over another; it also suggests that these tendencies emerge more forcefully after a failure or when the institution is under threat. Secondly, based on the data we have, we make judgements about which subsectors fit into which categories. On balance, we feel that the five subsectors do fit convincingly into the different categories and provide useful insight into each subsector, but also raise important questions about risk and vulnerability that require further research.

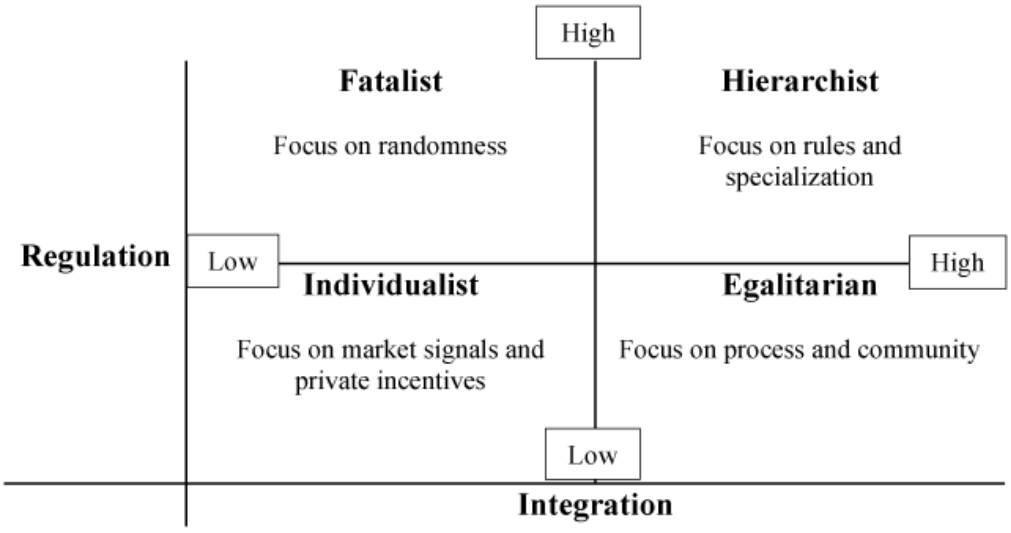


Figure 12: Cultural Theory typology

Application of Cultural Theory to the Five Subsectors

Within the transportation sector, airports have the most hierarchical tendencies. While airports are subject to market pressure, security is highly regulated in the sector, and key stakeholders are largely integrated into the process. Airports do not compete on the issue nor is the government or industry particularly transparent on the issue of security. Government leadership is also strongly committed to the issue of security. Airports also have more formal practices in place, which are typical of hierarchical arrangements, such as formal agreements with emergency services and specific pre-ordained security processes to follow.

We also place rail in this category though its hierarchical tendencies are not as pronounced as the airports. Rail is subject to considerable market pressure—two of the Class 1 rail carriers are competitive, raise money on private markets and report to their shareholders. Notwithstanding these competitive pressures, the sector is not atomistic and dynamic in the way the trucking industry is, for example. Class 1 rail carriers are large organizations, sub-divided, specialized and highly regulated, like any bureaucracy; dramatic changes take time. Historically and to the present day, rail infrastructure is strategic at the national level, and governments therefore take an active interest in Class 1 rail carriers. Interactions between government and industry have corporatist characteristics, which is to say they are privileged, non-competitive and significantly influenced by a few large firms. These large firms also have influence through the sector as a whole. In addition, government still has considerable direct influence on VIA Rail.

According to Cultural Theory, the hierarchist (high regulation/high integration) understands good governance to mean a stable and predictable environment (Hood, 1998: 75). On the positive side, a smaller number of bigger organizations—typical of a hierarchical arrangement—can be easier to organize. This dynamic could work particularly well in airports and rail, where a handful of large organizations dominate. Due to its size, this organizational design is also the most similar to government bureaucracies and therefore is conducive to a stable relationship with government regulators. While these organizations may take different strategic directions due to competitive forces, their size and importance mean they rarely go out of business, which further protects the stability of the sector. Their considerable resources allow them to secure expertise when required. Generally, these sectors are likely to enjoy stable, trusting and collegial relationships with government regulators, which can facilitate consensus on risk management priorities for the sector (Vogel, 1986).

Hierarchists have blind spots also. They have a highly optimistic view of management; when things go wrong they generate more standards, recruit experts and engage in formal strategic processes, which are criticized for being overly rational (Hood, 1998: 53). Such sectors can be loath to accept dramatic change unless all interests believe it is warranted or there is a profound external shock to the system; they are not known for their flexibility. When things go wrong, hierarchists blame lack of expertise and strategic thinking. The organizational type can ‘over’ regulate its staff and in so doing diminish adaptive or innovative behaviour. Despite the effort to

make reporting relationships clear, hierarchical systems are susceptible to people working at cross-purposes. Similarly, the vastness of the typical hierarchy allows members to react slowly, absorb significant resources and sweep indiscretions 'under the rug.' Because larger players dominate, rules are developed with them in mind. Smaller players are too often regulated in the same manner as the bigger players; nuance is not the strong suit of the hierarchist.

Their strength lies in their potential for strong leadership, stability, extra human and financial resources and ability to secure expertise. To enhance security practices, these types of organization should work on flexibility and adaptive capacity. Arguably, airports, in particular, have already made some important progress in this respect but more can be done. Leadership must continue to focus on improving security practices. It can do this by borrowing from the more commonly accepted and regulated safety practices but must also by encouraging a culture of transparency and learning throughout the organization. In addition to following the rules, staff must also be encouraged to apply sound judgement in complex situations. Often staff are blamed for not following rules, which can hamper a learning environment; there is too little attention paid to the context in which the decisions are made and the actual outcome of events. Finally, leadership must refine its approach to security such that smaller, low-risk operators are given appropriate flexibility while being held to an appropriate standard and to account for failures.

While unionized truckers would suggest a strong egalitarian tendency in certain contexts, we describe the sector here as individualistic due to the large number of SMEs, and their more pronounced sensitivities to market conditions, such as the price of oil and insurance as well as customer needs, which interview subjects in trucking stress more than others did. Many providers are local and hence the regulatory complexity across provinces is less important.

The individualist (low regulation/low integration) understands good governance to mean minimal rules and interference with free market processes. Individualists believe that people are self-seeking, rational and calculating opportunists. Individual responsibility rules supreme and apathy means consent (Thompson *et al.*, 1990: 34, 65). In contrast, individualists understand risk to be government regulation of the economy. For this type, competition is natural; companies will choose different risk management options based on return on investment. They do not see risks in isolation: the cost of mitigating risks will be weighed against the consequences of failures, as well as opportunities to exploit risk for private gain and the costs of risk management investments. Individualists are not motivated by the public interest. Trucking is highly atomistic; this will allow the subsector to be responsive in a CI event provided its private interests are also served and there is sufficient capacity available to serve the public's needs. Unlike the other subsectors, individual operators can much more easily go out of business with less disruption to the subsector or the economy; as a result trucking can be considered more adaptive and resilient.

Despite the individualist's faith in market practices, individualist practices such as pay-for-performance can undermine collective goals and lead to competition, not cooperation. At the same time, because trucking is less well organized compared to the other subsectors, it is less

likely to be an effective lobby, which means standards are easier for government to impose but consultation and reliable information-gathering is harder to conduct. They are also much more immediately sensitive to price signals. While on the one hand this means appropriate incentives can drive desired behaviours, it also means that this subsector will be more sensitive to cost increases, such as in the price of oil. The vast number of operators working in such a competitive context and with little direct oversight means it will also be difficult to capture those breaking the law for private gain.

Incentivizing better security practices by offering faster clearances at borders is a clever strategy and plays to trucking's individualist nature. Security practices can be improved by strengthening the incentive structure for security; higher and stricter standards as demanded by their clients, for example, can encourage this behaviour. Government might also work closely with the trucking industry groups to understand how to collect more reliable information from a sector that is highly dispersed and how best to coordinate it during a CI event. Government can also ensure it has a strong sense of how to move goods in and out of communities during events, including alternative routes, and how to communicate this information efficiently to the trucking sector. Natural disasters and industrial failures can block main arteries and critical supplies from arriving in a timely manner.

Bridge staff tend towards egalitarianism. There is a strong sense of 'team' or 'community' among those who are responsible for bridge infrastructure. Many bridge masters around the world know one another personally. They also share similar technical training. In contrast to the other subsectors, bridge staff are less inclined to spend their time expanding their external contacts outside the bridge community and more inclined to spend their time learning about the technical infrastructure for which they are responsible.

The egalitarian (high integration/low regulation) understands good governance to mean local, communitarian and participative organizations. For egalitarians, authority resides with the collective. Moreover, organizations are flat, or at least there is minimal difference between top officials and rank and file. Egalitarians understand risk to mean hierarchies and organizations outside their system. When things go wrong, egalitarians blame externals: 'management,' 'the executives,' 'the system' (Thompson *et al.*, 1990).

Bridge staff are keenly aware of the crucial role they play in connecting communities and supply chains. Notwithstanding this awareness, the theory suggests that bridge staff would tend to be inwardly accountable—to their team and to the profession of bridge masters. We feel there is supporting evidence for this predisposition. There is a high level of commitment to the team and its mission; as a result, the safety and security of the bridge will be taken seriously. Information gathering, standard setting and behaviour modification are not necessarily resisted in such a community but who delivers the message and how it is delivered are important. Egalitarians are much more likely to learn and adapt based on lessons emanating from specialists within their own subsector. Generally, this predisposition can be effective because risks associated with

bridges are often highly technical risks which bridge masters and industrial engineers are best placed to address. The 'team' thinking that is prevalent within egalitarian communities can sometimes get in the way of more innovative behaviour and making new connections beyond their immediate network. Changes can be slow; rules are often informal and not always apparent to outsiders. If organized on too large a scale, it is susceptible to breakdowns and fracturing.

Security practices can be enhanced by encouraging greater outreach into the broader community, including other critical sectors and communities outside the transportation community and emergency services. Egalitarian organizations can encourage innovative approaches to security by developing team-based rewards for good ideas and can benefit from scenario planning that tests their ability in non-routine events. Finally, the informality of the subsector can make it opaque; bridge staff should formalize security practices and thereby make them more transparent, teachable and transferrable.

Seaports are regulated but isolated, and as a result most closely exemplify the fatalist tendencies. Seaports do not see themselves as private organizations nor do they feel as though they are part of government. They express the most frustration that they are left out of the security community. The market pressures that they (and those businesses in the port) face conflict with what they describe as unpredictable interactions from government. Despite the international nature of shipping, seaports do not identify with a port community. Unlike bridge staff, seaport staff usually feel little connection—only competition—between ports. Unlike airports in which there is a strong sense of cohesive leadership nationally and internationally on security, seaport staff feel decision-making is highly fragmented, and unpredictable. The lack of seaport security and stable governance in parts of the shipping world creates further uncertainty for them.

The least-studied type (Hood, 1998), and perhaps the one with the most to offer on resilience, is fatalism. Fatalists suggest that plotting and planning for all hazards is an act of hubris. For fatalists, there is too much complexity and interdependence; our reporting mechanisms cannot anticipate all failures and bureaucracies are insufficiently responsive. For the fatalist, good governance anticipates lack of cooperation between stakeholders in a chaotic and unpredictable universe (Thompson *et al.*, 1990: 35).

The randomness that makes up fatalist forms of governance undermines the incentive to build strong teams. Unlike the hierarchist who is optimistic about management potential, the fatalist is skeptical. Not surprisingly, interview subjects from the seaport sector question the accuracy of information, doubt many of the standards, and recognize that as the wind blows so must their behaviour change. Due to the problematic nature between cause and effect for fatalists, they are least likely to plan in advance of a hypothetical event. Because they feel vulnerable, they are unlikely to take drastic actions if required because they may not feel as though after-the-fact their overseers will support the decisions they made in the event.

Security practices can be enhanced by integrating the seaports more fully into the security community of practice. This requires normalizing the relationship between the seaports and key stakeholders, including with security agencies and other CI sectors upon which the seaports rely, with an eye to enhancing trust between themselves and key players. Seaports also require a clearer sense of the importance of security in relation to competing market priorities; this requires stronger leadership with a more clearly articulated vision of where security fits in a competitive market context. Their skepticism can be a strong point; they are unlikely to accept that plans are foolproof and this perspective can be healthy in CIP and emergency management. Their skepticism can, however, overwhelm their surge capacity in a crisis; scenario planning that tests their ability in non-routine events would be helpful. Finally, encouraging a stronger sense of community among Canadian seaports might facilitate the sharing of best practices, and the benefits of a stronger sense of community as we have seen among bridge masters.

The figure in Appendix 5.3 summarizes this discussion.

In sum, Cultural Theory helps to identify different institutional arrangements in the subsectors and suggests their preferred forms of governance and associated strengths and weaknesses. At times, the characterizations may seem extreme; however, the theory allows us to organize a discussion of the sector, and place the subsectors in relation to one another. It allows us to see how each subsector will place a different emphasis on information gathering, standard setting and behaviour modification. In addition to highlighting the potential strengths and weaknesses of the preferred arrangements of each subsector, it also highlights the quite different characteristics of each subsector, and in so doing, the difficulty of coordinating within the sector as a whole. Blanket transportation policies would seem to have little chance of success. Cultural Theory highlights one must bring a more nuanced understanding of each subsector to the fore when attempting to regulate risks.

5.0 Conclusion

Standing at the ready for low-probability/high-consequence events can rarely be justified in market terms. We find that when subsectors experience less competition and regulatory complexity and stronger incentives and organizational commitment to enact security, security practices are more robust. In many instances, however, security competes with a number of market and cultural/institutional pressures.

At the same time, it is a highly volatile policy space. The media amplify disasters and the public has a fascination with them and an aversion to them. In this sense, having a strong information-gathering capacity in place is a necessary but not adequate condition for government regulatory regimes. As CI is critical to our collective social and economic needs, government must develop—however deftly—capacity for enacting standards and behaviour change without being an unnecessary drain on these sectors. While focussing on the unique characteristics of specific events is important, emphasizing best practises in business continuity more generally will likely generate more traction in the business community than focussing too much on specific low-probability events. More progress on transparency, accountability, prioritization, redundancy and adaptive capacity will help; so too will a strong sense of purpose guided by liberal democratic values. The approach will be more effective if underpinned by an understanding of the unique contextual influences in each subsector, and how the subsector connects to and supports the goals of the transportation sector as a whole.

5.1 Appendix I: Methodology

In 2011 and 2012 and with the support of SSHRC funding, we conducted and transcribed 55 semi-structured interviews with CI regulators, owners, operators and managers. Of the interviewees, 38 possessed expertise managing risk and security in the transportation sector. In 2013 and following the support of the Kanishka project, we conducted an additional 12 interviews with regulators, owners, operators and managers from the transportation sector with experience relating to security. Most interviews were audio recorded and all were fully transcribed. The interview tool was designed to extract data that relates to the Hood *et al*. (2001) risk regulation regime framework. The tool and process were approved by Dalhousie's Research Ethics Board. As part of our commitment to the Board and our research subjects, transcripts are confidential and exact quotations are not used without the explicit permission of the interview subjects.

A mixed-method analysis was conducted on the interview data, consisting of both quantitative and qualitative methods. The quantitative analysis consists of descriptive statistics, including simple means and response percentages. The small sample size of interview subjects in any one subsector would preclude the use of any rigorous statistical analysis to support generalizations of the findings. At the same time, we have found it useful when conducting semi-structured interviews to ask interview subjects to score contextual pressures that influence how they spend their time, for example. While not generalizable, the scoring allows interview subjects to distinguish more succinctly the impact of the different pressures. It also allows us to rank and compare how individuals perceive the different pressures. We present the data as indicative of the relative importance of the contextual influences as assessed by these individual interview subjects and use it as a point of departure for analysis and discussion. In almost all cases, the scoring was supplemented by extensive discussion with the interview subjects. It should also be noted that we conducted a number of interviews with executive-level public officials who had an over-arching responsibility for transportation as a whole and, therefore, offered views about contextual pressures in transportation as a whole but did not necessarily score contextual pressures for individual subsectors.

We used a grounded theory-based approach to extract and organize additional themes. We used a software package, Leximancer, to identify common themes in the interviews. We then reviewed the interview scripts based on themes and according to concepts germane to the framework. We supplemented this work with a comprehensive literature review of research on the regulation in the transportation sector. Towards the end of the drafting process, we also attended an international transportation security conference and asked a senior scholar with expertise in the transportation sector to comment on a late draft.

Media Analysis

We reviewed 1857 newspaper articles from four different newspapers; 1199 were about H1N1 in particular, which were removed from our analysis here. We accessed the coverage of these events by using the Factiva database to search within a leading national newspaper in each country: the *Australian*, the *Globe and Mail*, the *Daily Telegraph* and the *New York Times*. These are all high-distribution newspapers and opinion leaders in each of the respective countries. We identified our sample by drawing on all articles that appeared in the period of one year following the date at which each event began and that included in the article the term(s) most commonly used to refer to the event. We eliminated any articles that were clearly not principally about the event. These types of events tend to appear in large numbers of articles during the year in which they occurred, for instance, but the references to the events are often 'asides' in articles that are principally about something else.

For analysis of the content of the articles, we counted the number of articles that referred to various key terms. The key search terms were selected based on conventional items that were relevant to public administration and risk management. We also determined whether key actors—such as government and owners and operators in critical sectors—were assessed positively, negatively or neutrally. (N/A was also an option.) To summarize the performance data, a value of +1 was assigned to each article that was on balance a positive assessment for each key sector; a value of -1 to each article that was on balance a negative assessment, and neutral assessments were given 0. We then calculated the total net sum, adding the number of positive and negative assessments together. When assessing government performance, each order of government was assessed separately. In other words, if one article has a negative assessment of both the federal and provincial government, then it is assessed -2.

All non-H1N1 articles were analyzed during February and March 2010. We reduced the impact of the bias in assessments by using several strategies. As noted, we assessed all the articles during a short and fixed period of time. We also developed a standard template and applied it to all articles. All results were stored in a Microsoft Access database that we developed and maintain. Four research assistants classified all non-H1N1 articles—one each for the *Australian*, the *G&M*, the *Daily Telegraph* and the *NYT*. The group met at the start and periodically to review articles together to reinforce some level of consistency. Finally, a fifth research assistant coded independently 10% of the articles, as noted below.

Inter-rater Reliability

To test the inter-rater reliability of all aspects of coding, 10 per cent (n=186) of the 1857 articles were coded independently of the original coders. Using Cohen's kappa coefficient we found an inter-rater reliability agreement of k = .66 for government performance assessment. This corresponds to a reasonable level of agreement.

5.2 Appendix II: Interview Participants

Table 2: List of Interview participants

Role	Sector	Code	Date
Industry Association	Aviation	Int 1	Dec-2011
Owner/Operator/Manager	Bridge	Int 2	Sep-2011
Government Regulator/Official	Other	Int 3	
Government Regulator/Official	Ports	Int 4	Dec-2011
Owner/Operator/Manager	Rail	Int 5	Jul-2011
Owner/Operator/Manager	Rail	Int 6	Nov-2011
Owner/Operator/Manager	Surface Transport	Int 7	Jul-2011
Industry Association	Surface Transport	Int 8	Jun-2011
Owner/Operator/Manager	Surface Transport	Int 9	Jul-2011
Industry Association	Aviation	Int 10	Feb-2012
Government Regulator/Official	Aviation	Int 11	Sep-2011
Owner/Operator/Manager	Aviation	Int 12	Oct-2011
Owner/Operator/Manager	Aviation	Int 13	Oct-2011
Owner/Operator/Manager	Aviation	Int 14	Feb-2012
Industry Association	Aviation	Int 15	Aug-2013
Owner/Operator/Manager	Bridge	Int 16	Jun-2011
Owner/Operator/Manager	Bridge	Int 17	Nov-2011
Owner/Operator/Manager	Bridge	Int 18	Sep-2011
Owner/Operator/Manager	Bridge	Int 19	Aug-2011
Government Regulator/Official	Other	Int 20	Jan-2012
Government Regulator/Official	Other	Int 21	Aug-2011
Government Regulator/Official	Other	Int 22	Dec-2011
Government Regulator/Official	Other	Int 23	
Government Regulator/Official	Other	Int 24	Oct-2011
Government Regulator/Official	Other	Int 25	Aug-2011
Government Regulator/Official	Other	Int 26	Oct-2011
Government Regulator/Official	Other	Int 27	Mar-2012
Government Regulator/Official	Other	Int 28	Nov-2011
Transportation Specialist	Other	Int 29	Jul-2013
Owner/Operator/Manager	Ports	Int 30	Jun-2011
Owner/Operator/Manager	Ports	Int 31	Aug-2011
Owner/Operator/Manager	Ports	Int 32	Jul-2011
Owner/Operator/Manager	Ports	Int 33	Dec-2011
Owner/Operator/Manager	Ports	Int 34	Sep-2011

Industry Association	Ports	Int 35	Jul-2011
Industry Association	Ports	Int 36	Sep-2011
Government Regulator/Official	Ports	Int 37	Jul-2011
Government Regulator/Official	Ports	Int 38	Jul-2011
Government Regulator/Official	Other	Int 39	Sep-2011
Government Regulator/Official	Ports	Int 40	Aug-2011
Owner/Operator/Manager	Ports	Int 41	Jul-2013
Owner/Operator/Manager	Ports	Int 42	Jul-2013
Government Regulator/Official	Other	Int 43	Aug-2013
Government Regulator/Official	Other	Int 44	Sep-2013
Owner/Operator/Manager	Rail	Int 45	Sep-2013
Government Regulator/Official	Other	Int 46	Aug-2013
Government Regulator/Official	Other	Int 47	Aug-2013
Transportation Specialist	Ports	Int 48	Jul-2013
Government Regulator/Official	Surface Transport	Int 49	Jul-2013
Government Regulator/Official	Other	Int 50	Aug-2013

*Other includes emergency managers, and senior and management level government officials in transportation (not subsector specific).

Table 3: List of interview participants by sector and type

Sector	**Regulator**	**Owner/Operator/Manager**	**Industry Association**	**Expert/Academic**	**Total Number of Interviews**
Aviation	1	3	3	0	7
Port	4	7	2	2	14
Bridge	0	5	0	0	5
Rail	0	3	0	0	3
Trucking	1	2	1	0	4
Other	16	0	0	1	17
Total					50

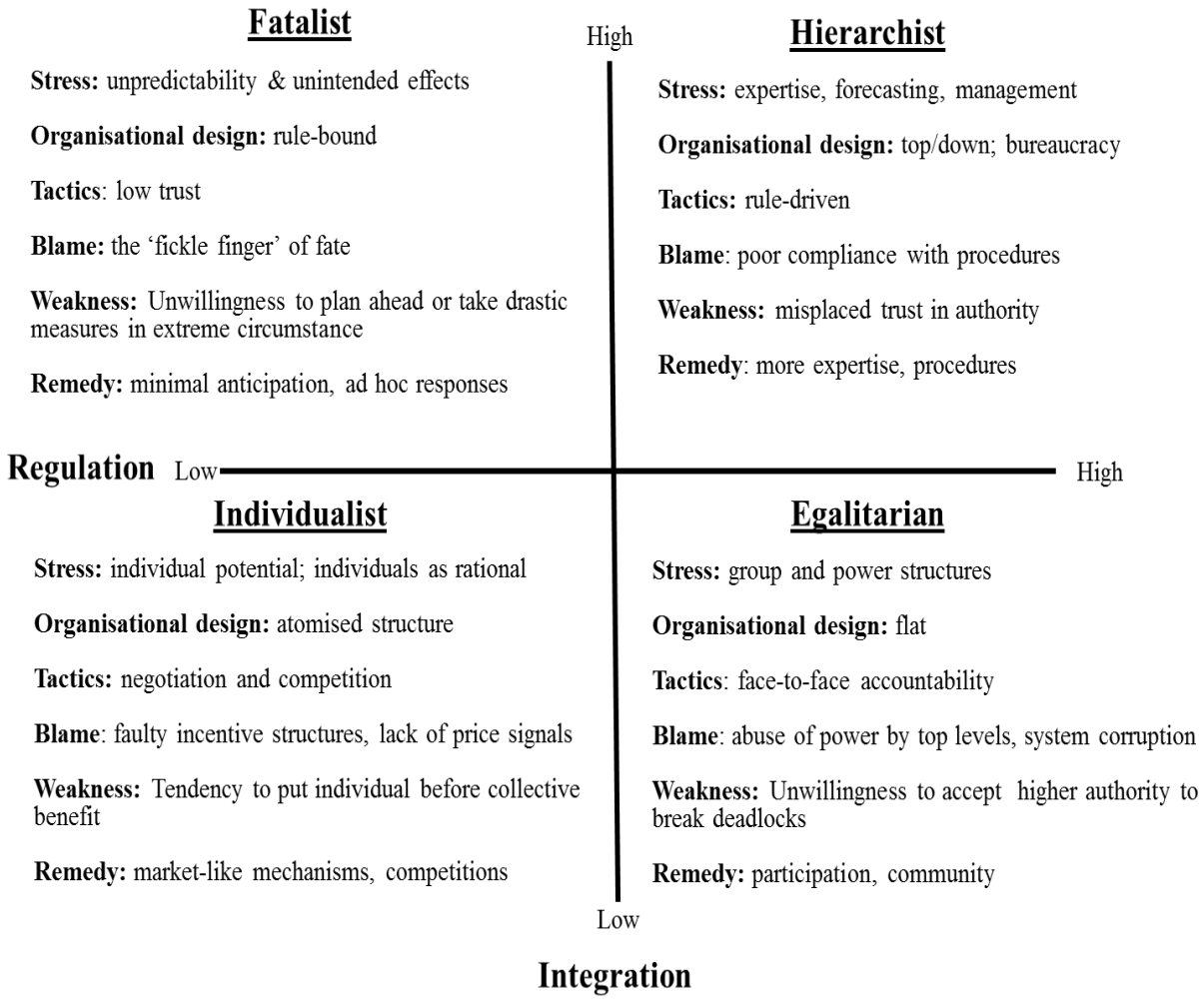
*Other includes emergency managers, and senior and management level government officials in transportation (not subsector specific).

5.3 Appendix III: List of Selected CI events for Media Analysis

Table 4: List of selected CI events for media coverage analysis

Food Safety	Maple Leaf Listeriosis Outbreak E. Coli Contamination of Spinach
Natural Disasters	Canberra Bushfires California Wildfires Hurricane Juan
Industrial Failure (Dangerous Chemicals)	Buncefield Explosion Toronto Propane Explosion Texas City Oil Refinery Explosion Melbourne Chemical Spill
Industrial Failure (Transportation Infrastructure)	Minneapolis Bridge Collapse (I-35W) Waterfall Train Accident Montreal Bridge Collapse (de la Concorde) Potters Bar Train Wreck
Failed Terrorist Plot	Transatlantic Flight Plot Sydney Five Toronto 18 Sears Tower
Cyber Attack	Estonia Cyberwarfare (2007) Albert Gonzalez (hacker fraud) CRA Software Defect (2007) Conficker Computer Worm Ghostnet SQL Slammer Computer Worm

5.4 Appendix IV: Cultural Theory Summary



Adapted from Hood (1998)

5.5 Appendix IV: Notes about the Authors

Kevin Quigley is the director of the School of Public Administration and the Principal Investigator of the CIP Initiative at Dalhousie University, Halifax, Canada.

Bryan Mills is a recent graduate of the MPA program at Dalhousie and is a research assistant for the CIP Initiative at the School of Public Administration. He is currently studying law at the University of New Brunswick.

6.0 Works Cited

Australia. Attorney-General's Department (2003). Trusted Information Sharing Network [website].Retrieved from http://www.tisn.gov.au/Pages/default.aspx.

Alhakami, A. S., Slovic, P. (1994). A psychological study of the inverse relationship between perceived risk and perceived benefit. *Risk Analysis*, 14(6), 1085-1096.

Boardman, M. (2005). Known unknowns: The illusion of terrorism insurance. *Georgetown Law Journal*, 93, 783.

Brooks, M. R. (2008). *North American Freight Transportation*. Northampton, MA: Edward Elgar Publishing Ltd.

Brooks, M. R. (2007). Port devolution and governance in Canada. *Research in Transportation Economics,* 17, 237-257.

Brooks, M. R. (2004). The governance structure of ports. *Review of Network Economics,* 3(2), 68-183.

Brooks, M. R., Prentice, B. (2001). Airport devolution: The Canadian experience. In *Seoul, Korea: World Conference on Transport Research,* July.

Brown, T. R., Hatch, A. B. (2002). The value of rail intermodal to the U.S. Economy. Retrieved from http://intermodal.transportation.org/Documents/brown.pdf

Burges, D. (2012). *Cargo Theft, Loss Prevention, and Supply Chain Security*. Butterworth-Heinemann.

Canadian Aviation Regulations (2012). Retrieved from http://www.tc.gc.ca/eng/civilaviation/regserv/cars/menu.htm

Canadian Border Services Agency (2013a). Free and Secure Trade. Retrieved from http://www.cbsa-asfc.gc.ca/prog/fast-expres/

Canadian Border Services Agency (2013b). Partners in Protection (PIP). Retrieved from http://www.cbsa.gc.ca/security-securite/pip-pep/menu-eng.htmlCanadian Trucking Alliance (2012). Snapshot of Trucking Industry. Retrieved from http://www.cantruck.ca/iMISpublic/Content/NavigationMenu2/CTAIndustry/TruckinginCanada/default.htmlois.justice.gc.ca/eng/regulations/SOR-96-433/

Caruson, K., MacManus, S. (2011). Gauging disaster vulnerabilities at the local level: Divergence and convergence in an 'all-hazards' system. Administration & Society 43(3), 346-71.

Centre for the Protection of National Infrastructure (2006). *CPNI* [website]. Retrieved http://www.cpni.gov.uk/

Cobb, R. W., Primo, D. M. (2003). *The Plane Truth: Airline Crashes, the Media, and Transportation Policy*. Washington, DC: Brookings Institution Press.

Cohen, B. C. (1983). *The Press and Foreign Policy*. Westport, CT: Greenwood Press.

C-TPAT (2013) C-PAT program overview. Retrieved from http://www.cbp.gov/linkhandler/cgov/trade/cargo_security/ctpat/ctpat_program_information/what_is_ctpat/ctpat_overview.ctt/ctpat_overview.pdf

Dake, K. (1991). Orienting dispositions in the perception of risk an analysis of contemporary worldviews and cultural biases. *Journal of Cross-Cultural Psychology*, 22(1), 61-82.

Douglas, M. (1982). *In the Active Voice*. London: Routledge.

Douglas, M. (1992). *Risk and Blame: Essays in Cultural Theory*. Routledge.

Douglas, M. (2001). Dealing with Uncertainty. The Multatuli Lecture. Leuven as cited in P. Hennessy (2010), *The Secret State: Preparing for the Worst* (1945-2010). London: Penguin.

Douglas, M., Wildavsky, A. (1982). How Can We Know the Risks We Face? Why Risk Selection Is a Social Process1. *Risk Analysis*, *2*(2), 49-58.

Environics Institute. (2002-06). *Environics Focus Canada 2002-06*. Queen's University, Canadian Opinion Research Archive [Distributor]. Retrieved from http://130.15.161.246:82/webview/.

Flynn, S. (2006). The brittle superpower. In P. Auerswald, L. Branscomb, T. La Porte, E. Michel-Kerjan (Eds.), *Seeds of Disaster, Roots of Response: How Private Action Can Reduce Public Vulnerability* (pp. 26-36). New York: Cambridge University Press.

Finucane, M. L., Slovic, P., Mertz, C. K., Flynn, J., Satterfield, T. A. (2000). Gender, race, and perceived risk: The 'white male' effect. *Health, Risk & Society*, 2(2), 159-172.

Forkenbrock, D. J. (2001). Comparison of external costs of rail and truck freight transportation. *Transportation Research Part A: Policy and Practice*, 36(4), 321-337.

Forsyth, P. (2007). The impacts of emerging aviation trends on airport infrastructure. *Journal of Air Transport Management*, 13(1), 45-52.

Hancioglu, B. (2008). The Market power of Airports, Regulatory Issues and Competition between Airports. German Airport Performance. Retrieved from http://userpage.fuberlin.de/~jmueller/gapprojekt/downloads/gap_papers/Hancioglu_Market_power_of_Airports_Regulatory_jul_08.pdf

Hainmüller, J. , Lemnitzer, J. M. (2003). Why do Europeans fly safer? The politics of airport safety in Europe and the U.S. *Terrorism and Political Violence*, 15(4), 1-36.

Hood, C. (1998). *The Art of the State: Culture, Rhetoric and Public Management*. Oxford: Oxford University Press.

Hood, C., Rothstein, H., Baldwin, R. (2001). *The Government of Risk: Understanding Risk Regulation Regimes*. Oxford, UK: Oxford University Press.

International Bridges and Tunnels Act (2007) Retrieved from http://laws-lois.justice.gc.ca/eng/acts/I-17.05/

Jenkins, B. M. (1998). Aviation security in the United States. *Terrorism and Political Violence*, 10(3), 101-111.

Johnson, B. B., Covello, V. T. (Eds.). (1987). *The Social and Cultural Construction of Risk: Essays on Risk Selection and Perception*. Dordrecht: Reidel.

Kahai, S. K., Ford, J. M. (1997). Economics of intrastate trucking regulation: Some empirical evidence. *Transportation Research Part E: Logistics and Transportation Review*, 33(2), 139-145.

Kahneman, D., Tversky, A. (1982). Rational choice and the framing of decisions. *Journal of Business*, 59(4), s251-s258.

Kearney, J. (2013). Perceptions of non-accidental child deaths as preventable events: The impact of probability heuristics and biases on child protection work. *Health, Risk & Society*, 15(1), 51-66.

Lindøe, P. H., Engen, O. A., Olsen, O. E. (2011). Responses to accidents in different industrial sectors. *Safety Science*, 49(1), 90-97.

Macdonald, A. (2014). Edmonton pipe bomb incident: How much power does airport security have? Retrieved from http://www.cbc.ca/news/canada/edmonton-pipe-bomb-incident-how-much-power-does-airport-security-have-1.2498105

Madore, O., Shaw, D. J. (1993) The Canadian airline industry: its structure, performance and prospects. Retreived from http://publications.gc.ca/Collection-R/LoPBdP/BP/bp329-e.htm.

Marine Transportation Security Act (1994) Retrieved from http://laws-lois.justice.gc.ca/eng/acts/M-0.8/

McCombs, M. (2005). A look at agenda-setting: Past, present and future. *Journalism Studies*, 6(4), 543-557.

Mutz, D. C., Soss, J. (1997). Reading public opinion: The influence of news coverage on perceptions of public sentiment. *Public Opinion Quarterly*, 61(3), 431-451.

Office of the Auditor General of Canada (2013). Fall Report of the Auditor General of Canada. Retrieved from http://www.oagbvg.gc.ca/internet/English/parl_oag_201311_e_38780.html

Pidgeon, N. (1997). The limits to safety? Culture, politics, learning and man-made disasters. *Journal of Contingencies and Crisis Management*, 5(1), 1-14.

Public Safety Canada (2009). *National Strategy for Critical Infrastructure.* Ottawa: Her Majesty the Queen in Right of Canada. Retrieved from http://www.publicsafety.gc.ca/prg/ns/ci/_fl/ntnl-eng.pdf.

Ouchi, W. G. (1979). A conceptual framework for the design of organizational control mechanisms. *Management Science,* 25(9), 833-848.

Quigley, K. (2013). "Man plans, God laughs": Canada's national strategy for protecting critical infrastructure. *Canadian Public Administration*, 56(1), 142-164.

Quigley, K., Quigley, J., Mills, B., Stallard, K. (2013). Analysis of selected print media coverage of two cases of failed terrorist plots: *The Australian*'s Coverage of the 'Sydney Five' (2005) and *The Globe and Mail*'s Coverage of the 'Toronto 18' (2006). CIP Initiative at Dalhousie University Working Paper Series. www.cip.management.dal.ca

Quigley, K., Quigley, J., Pond, E., MacDonald, C. (2012). Analysis of print media coverage of two cases of food contamination: *The New York Times* coverage of the 2006 E. coli contamination of spinach and *The Globe and Mail* coverage of the 2008 Maple Leaf/ Listeriosis Event. CIP Initiative at Dalhousie University Working Paper Series. www.cip.management.dal.ca

Railway Safety Act (1985). Retrieved from http://www.tc.gc.ca/eng/acts-regulations/acts-1985s4-32.htm

Renn, O. (2008*). Risk Governance: Coping with Uncertainty in a Complex World.* London: Earthscan.

Renn, O., Burns, W. J., Kasperson, J. X., Kasperson, R. E., Slovic, P. (1992). The social amplification of risk: Theoretical foundations and empirical applications. *Journal of Social Issues,* 48(4), 137-160.

Reniers, G., Pavlova, Y. (2013). Introduction: Why a book on game theory for safety within the chemical industry? In G. Reniers, Y. Pavlova (Eds.), *Using Game Theory to Improve Safety within Chemical Industrial Parks* (pp. 1-11). London: Springer.

Russell, D. and Simpson, J. (2010), Emergency planning and preparedness for the deliberate release of toxic industrial chemicals. *Chemical Toxicology*. 48: 171-176.

Royal Society (1992), *Risk Analysis, Perception and Management*. London: Royal Society.

Sandman, P. M., & American Industrial Hygiene Association. (2012). *Responding to Community Outrage: Strategies for Effective Risk Communication*. Fairfax, VA: American Industrial Hygiene Association. (Original work published 1993).

Savage, I. (2001). Transport safety. In D. A. Hensher. K. J. Button (Eds.), *Handbook of Transport Systems and Traffic Control*. Amsterdam: Elsevier Science.

Schmitter, P.C. (1977). Modes of interest intermediation and modes of societal change in Western Europe. *Comparative Political Studies,* 10(1).

Schneier, B. (2003). *Beyond Fear: Thinking Sensibly about Security in an Uncertain World*. Gottingen: Copernicus.

Seidenstat, P. (2002). Terrorism, airport security, and the private sector. *Public Administration Review,* 2(1), 275-291.

Sheffi, Y. (2005). *The Resilient Enterprise: Overcoming Vulnerability for Competitive Advantage*. Cambridge, MA: MIT Press.

Shore, J. J. (2008). *The legal imperative to protect critical energy infrastructure*. Canadian Centre of Intelligence and Security Studies. Ottawa.

Sjöberg, L. (1998). Risk perception: Experts and the public. *European Psychologist*, *3*(1), 1.

Sloan, E. (2012). Homeland Security and Defence in the Post 9/11 Era in D. McDonough (editor) *Canada's National Security in the Post 9/11 World: Strategy, Interests and Threats*. Toronto: University of Toronto Press.

Slovic, P. (2011). The psychology of intervention: Why we need a villain. *The Ottawa Citizen*, A10.

Slovic, P., Finucane, M. L., Peters E., MacGregor, D. G. (2004). Risk as Analysis and risk as feelings: Some thoughts about affect, reason, risk, and rationality. *Risk Analysis,* 24(2), 311-322.

Slovic, P., Fischhoff, B., Lichtenstein, S. (1982). Why study risk perception? *Risk Analysis*, 2(2), 83-93.

Soumerai, S. B., Ross-Degnan, D., Kahn, J. S. (1992). Effects of professional and media warnings about the association between aspirin use in children and Reye's syndrome. *Milbank Quarterly*, 70(1), 155-182.

Starr, C. (1969). Social benefit versus technological risk. *Science (New York.), 165,* 3899, 1232-1238.

Steinberg, T. (2000). *Acts of God: The Unnatural History of Natural Disasters in America*. Oxford: Oxford University Press.

Stewart, M. G., Mueller, J. (2011). Cost-benefit analysis of advanced imaging technology full body scanners for airline passenger security screening. *Journal of Homeland Security and Emergency Management,* 8(1)

Sunstein, C. R. (2003). *Why Societies Need Dissent*. Cambridge, MA: Harvard University Press.

Thompson, M., Ellis, R., Wildavsky, A. (1990). *Cultural Theory*. Westport, CT: Westview Press.

Transportation of Dangerous Goods Act. (1985). Retrieved from http://www.tc.gc.ca/eng/acts-regulations/acts-1992c34.htm

Transport Canada. (2011a). Audit of Aviation Security Regulatory Oversight April 2011, Retrieved from http://www.tc.gc.ca/eng/corporate-services/aas-audit-870.htm.

Transport Canada. (2011b). Transportation in Canada 2011. Retrieved from http://www.tc.gc.ca/media/documents/policy/Transportation_in_Canada_2011.pdf

Transport Canada. (2012a). Interdepartmental Marine Security Working Group. Retrieved from http://www.tc.gc.ca/eng/marinesecurity/partnerships-285.htm

Transport Canada. (2012b). Road Transportation. Retrieved from http://www.tc.gc.ca/eng/road-menu.htm

Transport Canada. (2013a). National Civil Aviation Security Program (CARAC), Retrieved from http://www.tc.gc.ca/media/documents/security/NCASP_FINAL_ENGLISH_%282%29.pdf

Transport Canada. (2013b). Program Activity Architecture 2011-2012, Retrieved from http://www.tc.gc.ca/eng/corporate-services/planning-paa-32.htm#s1.

Transport Canada. (2013c). Road Security. Retrieved from http://www.tc.gc.ca/eng/roadsecurity/menu.htm

Transport Canada. (2013d). National safety code 1987. Retrieved from http://www.tc.gc.ca/eng/mediaroom/backgrounders-b01-r118-1350.htm

Transport Canada. (2013e). Canadian Port Authorities. Retrieved from http://www.tc.gc.ca/eng/policy/acf-acfi-menu-2963.htm

Transport Canada. (2013f). Harper Government introduces *Administrative Monetary Penalties Regulations* to support the *International Bridges and Tunnels Act*. Retrieved from http://www.tc.gc.ca/eng/mediaroom/releases-2012-h084e-6815.htm

Tversky, A., Kahneman, D. (1973). Availability: A heuristic for judging frequency and probability. *Cognitive Psychology*, 5(2), 207-232.

United States Customs and Border Protection (2013). Customs-Trade Partnership Against Terrorism (C-TPAT). Retrieved from http://www.cbp.gov/xp/cgov/trade/cargo_security/ctpat/

United States Department of Homeland Security (2008). *One Team, One Mission, Securing Our Homeland: U.S. Department of Homeland Security Strategic Plan, Fiscal Years 2009–2013*. Washington, DC: GPO.

Vogel, D. (1986). *National Styles Of Regulation: Environmental Policy in Great Britain and the United States* (Vol. 242). Ithaca, NY: Cornell University Press.

Wahlberg, A. A., Sjoberg, L. (2000). Risk perception and the media. *Journal of Risk Research*, 3(1), 31-50.

Wason, P. C. (1960). On the failure to eliminate hypotheses in a conceptual task. *Quarterly Journal of Experimental Psychology*, 12(3), 129-140.

Wilson, J. Q. (1980). *The Politics of Regulation*. New York: Basic Books.

Zinn, J. O. (2004). Literature Review: Sociology and Risk. Working Paper. Retrieved from http://www.kent.ac.uk/scarr/publications/Sociology%20Literature%20Review%20WP1.04%20Zinn.pdf