Improving U.S. Transportation Infrastructure Resilience through Insurance and Incentives

Gina L. Tonn
The Wharton School
University of Pennsylvania

Jeffrey R. Czajkowski
The Wharton School
University of Pennsylvania

Howard Kunreuther
The Wharton School
University of Pennsylvania

March 2018
Working Paper # 2018-01

For submission to: *Geneva Papers on Risk and Insurance – Issues and Practices*

Risk Management and Decision Processes Center
The Wharton School, University of Pennsylvania
3730 Walnut Street, Jon Huntsman Hall, Suite 500
Philadelphia, PA 19104, USA
Phone: 215-898-5688
Fax: 215-573-2130
https://riskcenter.wharton.upenn.edu/

THE WHARTON RISK MANAGEMENT AND DECISION PROCESSES CENTER

Established in 1985, the Wharton Risk Management and Decision Processes Center develops and promotes effective corporate and public policies for low-probability events with potentially catastrophic consequences through the integration of risk assessment, and risk perception with risk management strategies. Natural disasters, technological hazards, and national and international security issues (e.g., terrorism risk insurance markets, protection of critical infrastructure, global security) are among the extreme events that are the focus of the Center's research.

The Risk Center's neutrality allows it to undertake large-scale projects in conjunction with other researchers and organizations in the public and private sectors. Building on the disciplines of economics, decision sciences, finance, insurance, marketing and psychology, the Center supports and undertakes field and experimental studies of risk and uncertainty to better understand how individuals and organizations make choices under conditions of risk and uncertainty. Risk Center research also investigates the effectiveness of strategies such as risk communication, information sharing, incentive systems, insurance, regulation and public-private collaborations at a national and international scale. From these findings, the Wharton Risk Center's research team – over 50 faculty, fellows and doctoral students – is able to design new approaches to enable individuals and organizations to make better decisions regarding risk under various regulatory and market conditions.

The Center is also concerned with training leading decision makers. It actively engages multiple viewpoints, including top-level representatives from industry, government, international organizations, interest groups and academics through its research and policy publications, and through sponsored seminars, roundtables and forums.

More information is available at https://riskcenter.wharton.upenn.edu/

Improving U.S. Transportation Infrastructure Resilience through Insurance and Incentives

Tonn, G.L., Czajkowski, J.R., Kunreuther, H.C.

For submission to: *Geneva Papers on Risk and Insurance – Issues and Practices*

Abstract:
Transportation systems are vital to the U.S. economy and our way of life, being responsible for the movement of people and goods locally, regionally, nationally, and internationally. Major disruptions to these transportation networks associated with natural hazards, man-made hazards, accidents, or infrastructure failure cause significant social and economic impacts. Risk management tools, including insurance and mitigation measures, can reduce these impacts as well as recovery times associated with disruptions, but existing evidence suggests they are lacking in many transportation systems. Through qualitative analyses we identify a number of barriers and opportunities to improving infrastructure risk management including the need for better data and metrics to support resilience. We then present recommendations for policy measures to facilitate improvements in transportation infrastructure resilience.

Key words:
Infrastructure resilience; insurance; transportation

1. Introduction

The U.S. transportation network is comprised of a wide range of infrastructure systems, including aviation, roads and bridges, inland waterways, ports, rail, and transit. These transportation systems are vital to the U.S. economy and way of life being responsible for the movement of people and goods locally, regionally, nationally, and internationally. For example, as of 2012 it is estimated that transportation (investments, purchases, employment, etc.) accounts for 9 percent of the $13.3 trillion U.S. gross domestic product (GDP), with total transportation assets valued at $7.7 trillion (Baylis et al. 2015).

U.S. investment in transportation infrastructure has lagged (Baylis et al. 2015). One out of every five miles of highway pavement is in poor condition, most locks and dams on the inland waterway system are well past their 50-year design life, 9% of bridges are structurally deficient, and transit systems suffer from a $90 billion rehabilitation backlog (ASCE 2017). Meanwhile, rebuilding costs following natural and man-made disasters are increasing due to a higher degree of urbanization and a huge increase in the value at risk (Kunreuther and Michel-Kerjan, 2011; 2013). In the future, we can expect more extreme weather events due to climate change and changes in risk associated with demographic and technologic change (Schwab et al. 2016). The emergent and continuously evolving nature of terrorism threats, cyber-threats and technological accidents raise additional concerns about the vulnerability of our lifeline infrastructure on which Americans and businesses depend. An increase in the value at risk in hazard-prone areas also impacts disaster recovery and costs (Lloyd's 2017a).

Public and private outlays to cover the restoration, repair, and losses associated with large-scale disasters are becoming unsustainable. Associated indirect costs to the regional economy increase when repairs to damaged infrastructure are postponed (Birkmann et al. 2016). These delays are generally due to a lack of disaster preparedness, planning, and funds, and have a direct and very serious impact on business interruption. The extent of damage and the speed of restoration are also critical determinants of how quickly a disaster stricken area recovers (Chang et al. 2014).

In this context, enhancing the resiliency of the U.S. transportation system to natural and man-made disasters is paramount. Sufficient insurance coverage of transportation systems to catastrophic risks is an important resiliency strategy: when disasters occur, insurance protection ensures that capital from insurance claims will be rapidly available compared to federal disaster relief which is often delayed for months or years. In addition to providing financial protection against disaster losses, insurance and other alternative risk transfer instruments can also serve as a market-based incentive mechanism to encourage investments in mitigation measures in return for reductions in insurance premiums.

The financial and insurance sectors can play an important role in generating a new value proposition for enhancing infrastructure resilience by: (i) informing and focusing attention on catastrophic risks, (ii) creating economic incentives for catastrophic risk reducing measures that address the vulnerabilities and consequences associated with those risks, (iii) providing funds through mitigation loans that support investments in mitigation that foster resilience, and (iv) rapidly providing insurance claims payments that support recovery when disasters occur.

Our research identifies barriers to and opportunities for creating a robust catastrophic risk insurance market for U.S. critical infrastructure systems. Using a methodology of qualitative analyses and interviews with a number of infrastructure risk managers and insurers, we show that critical infrastructure is currently underinsured in the U.S. due to disincentives and budget constraints. By characterizing the current state of insurance and risk management for transportation infrastructure systems, we develop recommendations for improving its resiliency through insurance and other risk transfer mechanisms.

The study objectives include 1) identifying the current practices in insuring transportation systems through mainstream insurance markets as well as via alternative risk transfer instruments; 2) identifying the current disincentives for investing in greater infrastructure resilience in transportation systems prior to and in the aftermath of large-scale disasters; 3) outlining ways that transportation infrastructure--- publicly and privately-owned systems-- can become insurable so as to leverage the ability of insurance to create incentives for risk mitigation and to speed up available funding for relief, recovery, and reconstruction after a major disaster; 4) developing recommendations as to how the public sector and private sector can best work together to develop metrics and insurable standards for advancing resilience; 5) examining the value proposition for the role of insurance in advancing greater resilience for lifeline infrastructure sectors.

Section 2 provides background on transportation infrastructure in the U.S., including various catastrophic events faced by the system and their aftermath, risk management, and insurance supply and demand. Section 3 describes the qualitative data and methods used in our study. Section 4 presents our key findings on needs for improving infrastructure resilience and insurance. Section 5 provides conclusions and recommendations.

2. Background

The transportation system in the U.S. has distinct modes, some publicly-owned and some privately-owned, transporting both passengers and freight. U.S. transportation infrastructure includes 4.1 million miles of highways, 140,000 miles of railroad, 12,000 miles of inter-coastal waterways used commercially, more than 5,000 public use airports, over 8,000 commercial waterway and lock facilities, 180 maritime ports, and 4,900 transit stations (Baylis et al. 2015). Some types of transportation infrastructure are typically publicly owned, like most transit and road systems. Other types are typically privately owned like rail and maritime freight transport. Commercial airlines are privately owned, while most U.S. airports are owned and operated by the government. Other transportation systems are quasi-public organization, such as Amtrak, which is a government-owned corporation providing passenger rail service in the U.S.

The interconnectedness of the different transportation modes is both a source of fragility and a source of resilience. In some cases, a disruption in one system leads to a disruption elsewhere --- for instance, a disruption in the transit system could prevent airport employees from reporting to work, causing a disruption in airport services. On the other hand, the interconnectedness of transportation systems can lead to resilience when one mode of transportation can be substituted for another that is constrained by a disruptive event. Varied risks, risk management strategies, and insurance contribute to the resilience of transportation infrastructure systems.

2.1 Risks and disruptions to transportation infrastructure

Transportation infrastructure is subject to several types of significant disruptions: terrorist attack, failure of infrastructure equipment, major accident that is often caused by human error, and natural disaster (Ortiz et al. 2009). Infrastructure risks are greatest for systems in areas prone to extreme events, located near climate-sensitive environmental features, or already stressed by age or demand (Wilbanks et al. 2012). Furthermore, few transportation infrastructure systems currently maintain any substantial level of excess capacity or redundancy (Leavitt and Kiefer 2006).

Various significant disruptions to transportation infrastructure along with residual effects and policy implications are described in Table 1.

Table 1: Examples of Transportation Infrastructure Disruptions and Outcomes

Disruption	Summary of Disruptions and Outcomes
Hurricane Maria, Puerto Rico (2017)	• More than 1,500 roads and bridges were damaged along with vast traffic signal outages. Damage to the air traffic control system hindered access to the island (Lazo 2017). • Damage slowed restoration access and supplies and stranded residents.
Boston Transit Shutdown (2015)	• Record snowfall resulted in power outages, breakdowns, and fires in transit system. • Economic impacts associated with days of complete closure and extensive delays (Baylis et al. 2015).
Superstorm Sandy, New York City (2012)	• Transportation systems including road, rail, and subway were damaged and out of service. • Ferry terminals suffered only modest damage; ferry transport played a large role in recovery. • Proactive steps were taken to refuel vehicles of ferry staff so that they could get to work; an app was used to allow direct fare payment; ferry service was added to replace several out-of-commission trains (Burke and Sipe, 2014). • Following Sandy, high-level actions by the federal government demonstrated an intensified focus on incorporating resilience improvements into the recovery process.
West Virginia Freight Derailment (2015)	• Freight cars carrying crude oil derailed due to a snowstorm. • Oil leaked into Kanawha River, causing water plant shutdown. • U.S. Dept. of Transportation issued new rules for rail cars carrying crude oil (Baylis et al. 2015)
Hurricane Katrina, New Orleans (2005)	• Little effort made to assist non-drivers in New Orleans evacuation. Neither public buses nor trains were deployed to evacuate people out of the city. • Many public buses remained parked in the city where they were subsequently ruined by the flooding.

	• The lack of transportation for non-motorists led to additional problems including costly and dangerous rescue efforts, health problems, and distrust of authority (Litman 2006).
Kobe Earthquake, Japan (1995)	• Port of Kobe suffered extensive damage. • Only 9 of 186 cargo handling berths were functional after the earthquake and all 35 container berths were damaged. • Recovery of port business did not follow the restoration of damaged port facilities. Losses were attributed to damage along with a drop in production and trade in the region associated with the earthquake. • Port lost market share to other Japanese ports and lost substantial shares of its transshipment traffic to other world ports (Chang 2000).
Northridge Earthquake, Los Angeles (1994)	• Four freeway routes closed due to bridge failures. • $1.5 billion of the $6.5 billion in total regional economic activity loss associated with the earthquake was attributed to transportation disruption (Chang 2003).
Hurricane Rita, Texas (2005)	• Many fuel stations in Texas ran out of gasoline because fuel truck drivers did not report to work. • Significant delays occurred at the two Houston area airports because more than 150 TSA screeners facing evacuation did not show up for work (Litman 2006).
West Coast port lockout (2002)	• Labor dispute caused lockout at 29 West Coast ports. • Cost US economy $4.7 to $19.4 billion (2002 dollars) due to resulting shipping delays throughout the U.S. freight transport system (Ortiz 2009)

As these examples demonstrate, disruptions to passenger transportation systems can create economic losses because employees are unable to get to work. People reliant on public transportation can be left in harm's way if transportation assistance isn't provided during a disruption for evacuation or for other urgent transportation needs.

Disruptions to freight transportation can have wide-reaching economic impacts, and prolonged disruptions can have long-term impacts on the economy of a region as in the case of the Kobe earthquake in 1995. Transportation disruptions can also impact other infrastructure systems that rely on fuel, supplies and employees that are critical to their operations.

2.2 Infrastructure Risk management

The first step in risk management for infrastructure systems is to identify and evaluate the likelihood of specific disruptions occurring and their expected impacts. Three general strategies can then be considered for managing the risk: avoid, control, or transfer/finance. Risk avoidance involves eliminating hazards or exposures that can negatively impact an infrastructure system. When risks cannot be avoided, they can be controlled through mitigation. For example, building redundancies into the system can serve to reduce the frequency or severity of losses. It is important that systems are up to the latest standards and codes, and that systematic checklists are in place for operators to follow in order to facilitate recovery of the system after an event.

After identified risks have been partially controlled, the residual loss can be transferred via financing mechanisms through three broad methods – insurance (including reinsurance), self-insurance, or pooling of risks (Kaddatz 1995). An optimal risk management strategy often relies upon multiple layers of risk transfer. These layers are self-insurance/mitigation, insurance, reinsurance and alternative risk transfer, and lastly, public sector aid or backstops. Self-insurance and mitigation include both savings and mitigation measures undertaken to reduce consequences associated with a catastrophic event. Traditional insurance provides financial protection for a specified risk. Reinsurance and other risk transfer mechanisms such as catastrophe (CAT) bonds are used to cover potential losses that exceed the amount that can be economically covered by traditional insurance. For truly catastrophic events, public sector backup may be necessary to cover losses that exceed the limits of the first three layers of risk transfer.

A risk management strategy will assess the benefit and cost trade-offs associated with various modes of risk transfer to cover potential damage now and into the future. Kaddatz (1995) discusses a number of benefit-cost factors related to the selection of insurance, self-insurance, and pooling. For example, self-insurance provides a high level of control over loss prevention and claims adjustment, but a low level of cost stability. Commercial insurance comes at a higher cost and provides lower levels of control over loss prevention and claims handling. However, commercial insurance often offers the advantage of risk management services. Insurers are experienced in identifying, analyzing, and modeling risks, and can often help their customers better understand risks and develop strategies to manage them (Kaddatz 1995). In addition, risk management strategies including emergency planning, insurance, and recovery planning are needed to reduce losses after a catastrophic event.

2.3 Insurance supply and demand for transportation infrastructure

Insurance plays a key role in the resilience of infrastructure systems by providing funds to enable restoration and recovery following a disruptive event. Many commercial insurance companies (e.g. AIG, Travelers, XL Catlin, FM Global) insure infrastructure systems, and types and amounts of coverage vary for different transportation systems since infrastructure owners require different insurance policies for different hazards they are facing (Kunreuther et al. 2016). System size, assets, and geographic location affect risks and insurance needs and infrastructure managers can choose from many types and amounts of coverage. For instance, terrorism insurance is purchased independently of flood or earthquake coverage with different deductibles, limits, premiums and exclusions for each risk. System characteristics also affect insurance needs and insurability. Some infrastructure entities may not qualify for insurance coverage if they have not undertaken the minimum mitigation standards established by insurers for the infrastructure to be insurable. For example, a transit entity might be required to implement pre-trip bus inspections and establish a labor safety committee in order to secure insurance (Kaddatz 1995).

On average, only about 30 percent of catastrophe losses have been covered by insurance over the past 10 years (Vajjhala and Rhodes 2015). A key factor driving this infrastructure insurance gap is the role of federal disaster assistance, as it discourages investments that will enhance infrastructure resilience. More specifically, when infrastructure managers are confident that federal funds will be made available to make them nearly financially whole after a disaster strikes, they have little economic incentive prior to a disaster to expend their own limited resources on mitigation measures, or to purchase (sufficient) insurance that would reduce their potential losses and facilitate the recovery process.

Moreover, this behavior will potentially be exacerbated if natural disasters fall below an infrastructure manager’s threshold level of concern amidst a host of other competing priorities. For many transportation infrastructure managers, risks related to extreme weather and natural disasters are at the low end of the worry spectrum (Travelers Risk Index 2016), whereas risks related to employee healthcare costs and benefits are rated as much more pressing. Consequently, another contributing factor related to the insurance gap is that transportation infrastructure managers focus on immediate safety and reliability risks connected to their mission, as opposed to longer-term natural disaster resiliency concerns that are inherently low probability events.

In setting the price of premiums, insurers take into account their administrative costs, cost of capital and an acceptable return to their shareholders. These costs are balanced against insurance regulation requirements and the need to keep the price reasonable in order to attract demand. Premiums on a given policy depend not only on the level of risk the insured faces but also on the degree of concentration of risks in given locations for an insurance company. For instance, the premiums for two transportation systems are likely to each be lower if they are thousands of miles apart than if they are located in the same geographical area. In the latter case the insurer could suffer losses from both systems should a hurricane hit that region, while the likelihood of both coasts being hit in a year by two disasters is much lower.

Insurance premiums might increase in the aftermath of a large-scale disaster whether or not the insured entity suffered a loss. If an insurer paid billions in claims, it would need to raise more capital the following year, likely at an increased cost since the price of reinsurance is likely to have increased (unless the market has significant excess of capital). In this regard, insured critical infrastructure often encounters contraction of their coverage after a catastrophe. Prior to the September 11, 2001 terrorist attacks, Chicago’s O’Hare Airport had $750 million of terrorism insurance coverage at an annual premium of $125,000. After the attacks, insurers offered the airport only $150 million of coverage at an annual premium of $6.9 million (in nominal 2002 prices). This new premium, if actuarially fair, implies the annual likelihood of a terrorist attack on O’Hare Airport to be approximately 1-in-22 ($6.9 million/$150 million), an extremely high probability. The airport was forced to purchase this policy since it could not operate without coverage (Kunreuther and Michel-Kerjan 2004). This insurance capacity contraction is an important element for critical infrastructure owners to anticipate when they build their financial resiliency strategy.

There are opportunities to change the role that public sector authorities and funding programs play in risk reduction and resilience. Cash-strapped recipients of Stafford Act assistance are often granted waivers from insurance purchase requirements when insurance premiums are considered unaffordable. An improvement could be to allow catastrophe bonds and risk reduction projects to count toward insurance-coverage compliance requirements in cases where traditional insurance purchase is infeasible. This would encourage some level of risk mitigation or insurance when traditional insurance coverage is unattainable due to high premium costs and budgetary limitations. Insurance can also be used as a driver for resilience projects by timing alignment with insurance procurement and project construction dates (Vajjhala and Rhodes 2015).

Overall, we find that the interaction of the demand-supply market forces needs to be better understood, along with the role of insurance and resiliency in transportation infrastructure.

3. Data and Methods

Our research investigates the role of insurance in providing financial protection against infrastructure damage of transportation facilities and in encouraging investment in loss reduction measures. We used two methods to collect data: (1) review of technical reports and literature relevant to infrastructure resilience, and (2) interviews with managers from the insurance and infrastructure sector. Importantly, we investigate which risk management practices are actually utilized in transportation infrastructure systems.

Government, infrastructure organizations and the insurance industry have produced reports that are highly relevant to the topic of transportation infrastructure resilience and insurance that we discuss in more detail in Section 4. Rakich et al. (2011) includes a survey of airport risk managers and their insurance practices and strategies. Lloyd's (2017b) describes infrastructure resilience needs from an insurance perspective including case studies and suggested means to enhance infrastructure resilience. Baylis et al. (2015) highlight the importance of understanding systemic risks associated with transportation infrastructure with a focus on emerging risks and provide recommendations for improving operational practice and investing in resilient infrastructure. Vajjhala and Rhodes (2015) describe the need for innovation in funding infrastructure resilience projects, suggesting alternative financing instruments for resilience projects. The U.S. Department of Energy (2013) examines the role that insurance can play in managing key risks in energy infrastructure, including emerging risks. It highlights the benefits of insurance for recovery and resilience and links energy to other infrastructure sectors, including transportation.

We also gathered information from our interviews with insurers, infrastructure managers and with experts in resilience of air transport infrastructure and cyber resilience for infrastructure systems (see Table 2).

Table 2: Summary of Interviewees

Title(s)	Organization Type	Transportation Areas
Insurance		
Head of corporate insurance partners	Reinsurance	
Manager of Transportation Services	Insurance broker	Maritime
Vice President – Risk Consulting	Insurance	Maritime
Sr. Director, Enterprise CAT strategy Sr. Vice President Catastrophe Risk	Insurance	Various
Infrastructure Managers		
Strategy and Sustainability planner Director of strategic planning and analyses Project Manager – Resilience Office of the General Counsel	Infrastructure	Transit (rail, subway, trolley, bus)
Sr. Manager of Risk Management	Infrastructure	Port (maritime and airport)
Environmental Engineer	Infrastructure	
Director of Risk Management	Infrastructure	Port (maritime and airport)
Director of Risk Management	Infrastructure	Rail
Sr. Program Officer	Research	Air transport
Professor	Research	Air transport

We developed two sets of questions: one for insurers and one for infrastructure managers (see Appendix A.) The questions for insurers focused on current offerings, barriers to catastrophe insurance and resilience for transportation infrastructure systems, risks insured, layers of risk transfer, changes to insurance offerings over time, cyber insurance and challenges in quantifying risk. The interview topics were tailored to reflect the expertise and characteristics of the interviewees and their companies.

Questions for infrastructure managers focused on insurance and risk transfer decisions, including types of coverage purchased, changes in coverage over time, barriers to improved resilience and risk transfer, post-disaster recovery including government funding for past events, and expectations for future governmental disaster funding, measures to reduce future losses including actions taken and planned, as well as financial strategies for future losses in relation to current and emerging risks.

The interviews provided a broad picture of the challenges associated with the demand and supply of insurance to cover infrastructure risks.

4. Results

The following themes were consistently identified as key needs for improving transportation infrastructure resilience, insurance products and uptake of coverage: 1) need for more and better data; 2) need for metrics to measure resilience; 3) need for research and focus on emerging risks; 4) impact of reliance on federal funding for disaster relief; 5) benefits of risk engineering services of insurance; and 6) insurance as a tool for resilience financing.

4.1 Need for better data

Data availability and accessibility are key for developing new insurance products and evaluating risk management and resilience measures. High quality data that characterizes the future are important since risks will be changing over time. Better data allows more accurate risk-based pricing of insurance. New and better data could enable alerts of potential losses before they occur, real-time damage assessments, faster claims processing, more automation, and more personalized insurance products and services (Lloyd's 2017b).

Data could also facilitate the development of multi-year insurance contracts although this requires predictive analytics and governance. Multi-year contracts provide security to the client, but the insurer faces the possibility of changing and newly emerging risks. Improved technology could lead to the development of dynamic insurance policies that reflect changes in a client's risk. In theory, with real-time data, coverage and costs could be regularly updated based on real-time conditions. Government could potentially help in this regard by undertaking or funding research and data collection to enable technology for real-time risk assessment. This data collection and aggregation is a challenge for individual firm which track and utilize their own loss data, but aren't able to access or aggregate data from across an industry due to competition between firms and anti-trust regulations.

One infrastructure manager noted that their geographic region tends to drive insurance pricing for earthquake risks, and that loss reduction measures that they might implement are not likely to be considered by insurers in reducing their premiums. With data improvements, risk based pricing could become more practical, thus driving resilience improvements. Another insurer noted that data warehousing and aggregation across industries could be a good role for the government to play.

4.2 Need for metrics

Metrics provide the policyholder and insurer a framework for measuring and improving resilience and for adjusting premiums to reflect risk. Like data, they are important to insurers and infrastructure managers for evaluating risk-reducing measures and for understanding necessary or important insurance coverage types and amounts. Using risk scores that classify a policyholder's risk and then charging a risk-based premium with deductibles can incentivize investment in risk-reducing measures. Insurers could also use their applicable expertise to offer services beyond this that could assist with risk reduction such as assisting in developing risk management strategies, quantifying the economic value of ecosystem services in reducing natural hazard risk (e.g. natural flood storage), emergency preparedness prioritization, guidance on enhancing infrastructure robustness and redundancy, and developing worst case scenarios. Suggested areas for metrics include: efficacy of natural defenses, degree of diversity, asset maintenance levels, emergency response times, levels of critical resources, and levels of independence of recovery services (Lloyd's 2017b).

Regulations can be helpful in enabling insurers to set standards that an infrastructure system needs to meet. For instance, California SB1953 requires hospitals to be capable of remaining operational after an earthquake and sets deadlines for improvements to facilities that do not meet earthquake resilience standards (Meade and Kulick 2007). This regulatory requirement can help in assessing a hospital's risks when designing an insurance policy.

4.3 Emerging risks

Emerging and non-modeled risks coupled with system interdependencies, present substantial challenges to insurance firms (Lloyd's 2017b). Emerging risks are associated with new or future threats, where there is limited knowledge about probability and potential losses (Renn 2014). Three key emerging risks discussed prominently in our interviews are climate change, cyber risk, and terrorism.

Climate Change: Global warming is expected to bring changes associated with temperature extremes, storm and precipitation intensification and the potential for sea level rise. The uncertainty associated with climate change and its impacts is a significant challenge to insurers who need to be able to quantify the risk to determine whether it is insurable and, if so, to set a risk-based premium. Infrastructure managers must assess and factor climate change risks into short-term and long-term planning and capital projects. Some studies on impacts of climate change to infrastructure have been completed such as a multi-year study by Amtrak to understand climate change risks and their impacts in the Northeast Corridor (Amtrak 2015).

Cyber Risk: The number of reported cyber incidents for transportation systems has sharply increased in recent years, as indicated on Figure 1 based on reported incidents as listed in the Advisen Loss database (advisenltd.com). As shown on Figure 2, the highest number of cases is reported in air transportation, followed by support activities for transportation and transit, which includes air traffic control, marine cargo handling, and motor vehicle towing. With the rising number of cyber incidents, the need and interest in insuring transportation systems against cyber incidents is also increasing.

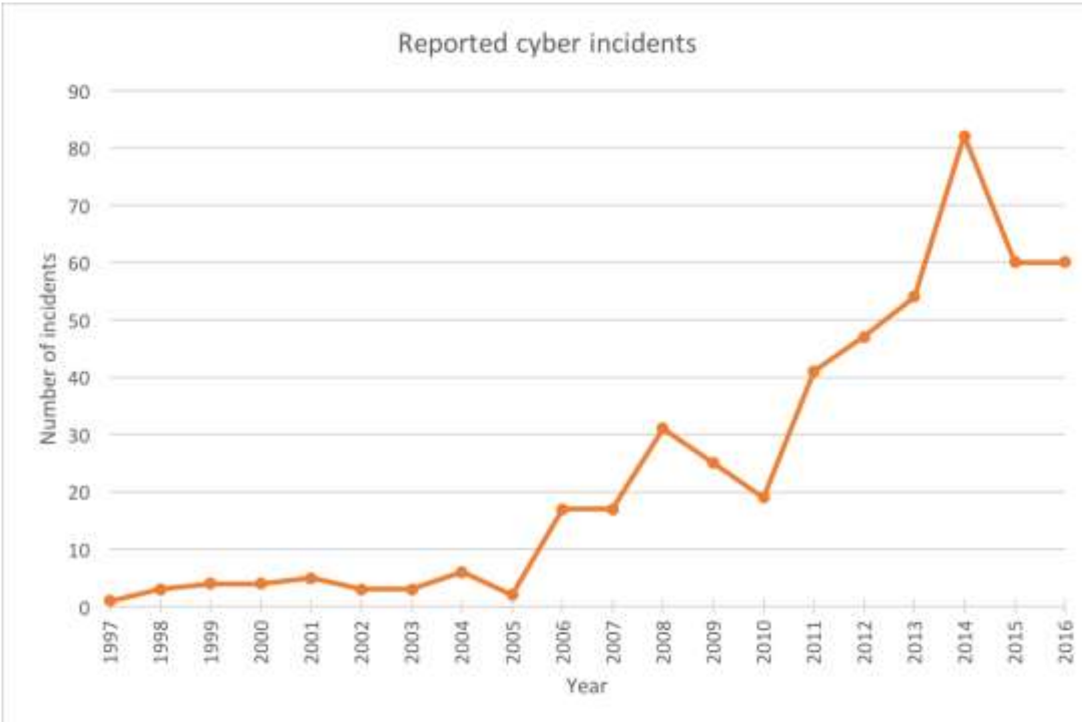

Figure 1: Number of transportation-related cyber incidents in the U.S.

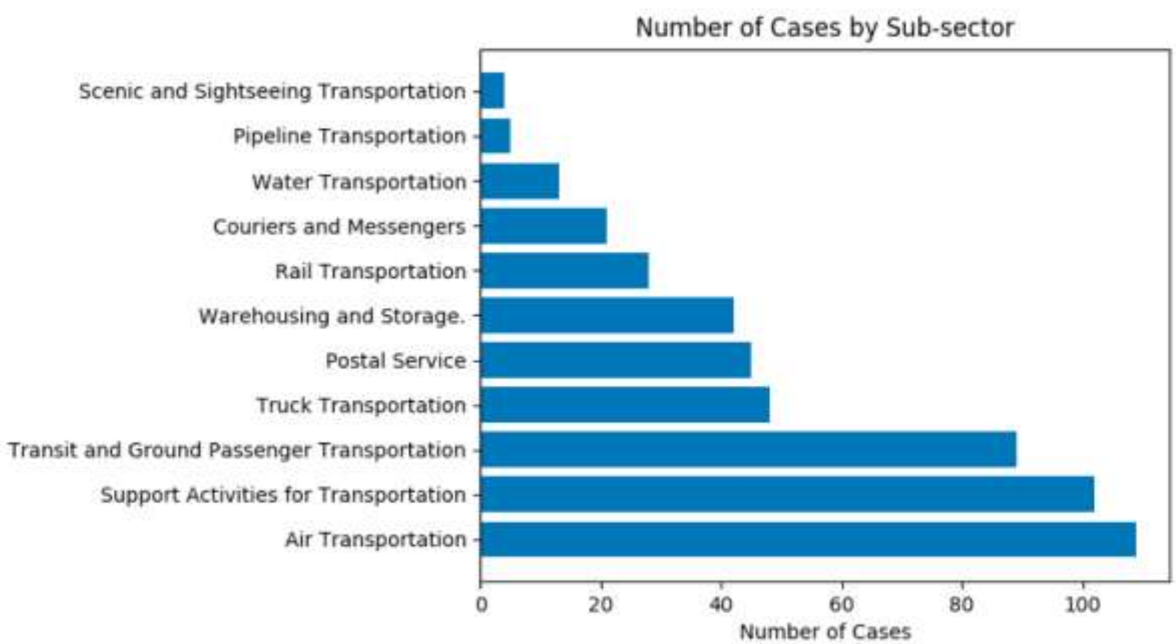

Figure 2: Number of cyber incidents by transportation sub-sector

While insurance coverage is available for cyber risk, it is difficult to access high coverage limits and there are limitations in available coverage. For instance, coverage associated with a data breach may not currently include reputational damage or business interruption. Insurers are reluctant to offer high limits (above $500 million) due to the aggregation of risk (Camillo 2017). The cyber-insurance market still needs to mature, and coverage is generally based on what the potential policy-holder is willing to pay, or on what other insurers are charging for similar policies. Data scarcity and information asymmetry are also issues with insurers having limited tools for assessing an infrastructure system's cyber risk (Kesan and Hayes 2017). Insurers are developing tools and methods for assessing cyber risk, including new scenario models and empirical models, which take advantage of information on past cyber events (Ng 2017). Government could play a role in setting standards for cyber risk management, which would both improve risk management and increase cyber insurance purchase. One such example is the California Data Breach Laws of 2003, which along with other legislation led to growth in cyber insurance. The U.S. National Institute of Standards and Technology (NIST) has been suggested as a provider of federal IT security standards. The forthcoming European Union General Data Protection regulation is expected to improve cyber security and increase demand for cyber insurance. (Woods and Simpson 2017, Camillo 2017). U.S. government agencies such as the Department of Homeland Security and the National Science Foundation can also support cyber resilience and insurance by continuing to fund research and development for technology to assess cyber risks, such as models and systems for data management and sharing.

A challenge for insurers of cyber risk is building a diversified set of policyholders to provide a balanced portfolio of risks that are not highly correlated with respect to future disruptions. There are no geographical boundaries to cyber risk, which means that a single cyber event could impact infrastructure systems around the world (Kesan and Hayes 2017). Pivotal cyber events could have far-reaching impacts, and insurance companies do not yet have a high enough confidence level to fully insure infrastructure systems against losses due to cyber risk. Insurers generally manage this correlation in risk through policy limitations and exclusions. As available data and models improve, insurers may better understand and manage correlations in cyber risk (Kesan and Hayes 2017).

One insurer indicated that they are undertaking vulnerability modeling for cyber risk and are developing a plan with infrastructure managers for managing this risk. Certain improvements in cyber security, such as password requirements, are relatively easy and inexpensive. Infrastructure managers can be made aware of these in the short term before addressing issues that require complex models.

Because cyber risk is still considered new and poorly understood, infrastructure managers want cyber policies with a broad range of coverage including breach reporting expenses, forensic expenses, penalties for credit card issues, ransomware, and business interruption due to hacking---areas that may be difficult for insurers to currently provide coverage.

Terrorism: The federal government under the Terrorism Risk Insurance Act (TRIA) provides a backstop for insurance claims related to acts of terrorism, but only applies to events certified as terrorism events by the federal government with aggregate losses exceeding $140 million in 2017 (Kunreuther et al. 2014). The program trigger is being increased by $20 million annually, up to $200 million for calendar year 2020 and thereafter. Given the required aggregate loss amount, some events such as the Boston Marathon bombing were not covered (Bonner 2017). Some infrastructure managers choose not to purchase coverage because events of most concern to their facilities would not be classified as terrorism under TRIA. Other infrastructure managers feel that terrorism risk is concentrated in urban areas, and choose not to insure for terrorism risk since they perceive their location not to be a target. One insurer indicated that 10 years ago, terrorism insurance was commonly purchased for infrastructure systems. Now, purchase rates are lower as companies are being selective in buying the coverage after undertaking cost-benefit analysis. In addition to excluding terrorism risk, standard commercial insurance policies generally exclude acts of war.

4.4 Reliance on federal disaster relief

Managers of publically owned transit and port systems that we interviewed indicated that they believe that the federal government would provide disaster assistance following a catastrophic event, and that federal support is a primary component of their risk management strategy. Insurers believe that the government's role is to assist in the recovery process after a catastrophic disaster. Furthermore, the insurance/reinsurance market is limited in the total amount of capital available to provide protection against catastrophic losses. Extremely high limits (>$5 billion) aren't feasible via insurance or excess coverage. One researcher indicated that resilience improvements are much more common in private infrastructure because they know that they cannot rely on the government as an insurer of last resort.

Under the Stafford Act, in order to be eligible for additional federal funding in the future, an infrastructure system must become insured after receiving disaster relief. One infrastructure manager noted that they were able to gain a waiver for this requirement at the state level due to the high price and limited availability of insurance as discussed in section 2.4. To further illustrate this point, in the aftermath of Sandy, the New York MTA could not obtain its previous insurance coverage of $1 billion; even $500 million in storm-surge coverage would have cost twice as much for half the amount of coverage that they previously had. The MTA had to use other risk transfer mechanisms, specifically a dedicated storm-surge $200 million catastrophe bond on top of its existing coverage for wind.

Primary reasons for not purchasing insurance are 1) affordability and 2) value (cost per amount of coverage). The insurer doesn't always have more informed knowledge of the risk than the client, which can lead to premiums that the infrastructure manager views as a poor value. The federal government or individual states could incentivize insurance purchase or mitigation (for example, with low interest loans for mitigation) to promote insurability and lower premiums.

4.5 Linking risk engineering and insurance

Insurers can use risk engineering (i.e., risk control) to help pinpoint the most cost-effective way for infrastructure systems to allocate their limited funds for resilience improvements. In addition to prioritizing mitigation spending, they can estimate how these measures will impact exposure and premiums. One insurer indicated that they use risk engineering to fine-tune coverage limits and to better understand exposure for pricing purposes. This risk engineering work enabled infrastructure managers to understand their exposure, undertake loss reduction measures and obtain insurance coverage at an attractive premium. On the other hand, another infrastructure manager noted that risk engineers from insurance companies aren't always as knowledgeable about risks to their infrastructure systems as they are.

4.6 Insurance as a tool for resilience financing

Insurance and reinsurance provide financial protection to policyholders so they are willing to undertake risk-related activities since they will be provided with funds for recovery when they suffer losses (Lloyd's 2017b). They can use insurance as a barometer for risk, with resiliency measured by the type and amount of insurance they can obtain. Infrastructure systems have limited budgets and funding. With aging infrastructure, it is often more practical to budget to replace these systems. Normally, insurance covers replacement after an event but does not cover upgrading damaged facilities.

Federal funding or loans are sometimes available for resilience improvements, but one infrastructure manager noted that they often don't use this funding because it doesn't cover 100 percent of their costs, and it is difficult to justify the required spending necessary to cover the remaining expenditures. Loans for resilience projects would help in this regard by enabling infrastructure managers to show a measurable return on investment.

5. Conclusions and Recommendations

After interviewing a diverse set of critical transportation infrastructure managers and insurers, it is clear that the extent of mitigation, insurance, and other risk management varies greatly as a function of budgetary constraints, type of system, and hazards faced. Enhancements to transportation infrastructure resilience and insurance are needed to address the challenge of increasing losses associated with catastrophic events. Based on the results of our study, we have generated the following seven recommendations on ways to address barriers to enhanced infrastructure resilience and insurance.

Recommendation #1: Consider Stafford Act revisions. Reliance on Stafford Act funding for catastrophic losses was noted as a key component of the risk management strategy for public infrastructure systems considered in this study. While the government is normally the insurer of last resort when a community suffers a catastrophic event, adjustments to the Stafford Act funding process could encourage improvements in infrastructure resilience and insurance coverage. One proposed revision to the Stafford Act (Establishing a Deductible for FEMA's Public Assistance Program 2017), which was presented for public comment in early 2017, is to require a disaster deductible to be met prior to the receipt of recovery funds (81 FR 3082). This deductible could be in the form of savings or through implementation of mitigation measures prior to a disaster. These types of modifications could encourage infrastructure managers to put additional focus on resilience. Other revisions could potentially allow for risk reduction measures to count towards insurance requirements when traditional insurance purchase is infeasible.

Recommendation #2: Promote alternative funding vehicles for pre-event resiliency investment linked to insurance premium discounts. Day-to-day operational and maintenance funding is scarce for many infrastructure managers who struggle with how to provide funding for longer-term resiliency efforts pre-event. Low interest loans could be an option that government could offer. While an infrastructure system might not be able to afford a $5 million resiliency improvement, with a 30-year loan at a 3% interest rate, their annual cost would be about $250,000, which could be affordable. Insurance-linked securities could also fund resilience measures. The affordability could be enhanced by reduced insurance premiums associated with the resiliency measure where applicable.

Recommendation #3: Facilitate catastrophic risk data collection, availability, and analysis. Insurers and infrastructure managers alike noted the difficulty in relating resilience improvements to insurance premiums and cost savings. High quality data acquisition, sharing, and analysis are needed to enable quantification of the benefits associated with resilience improvements. Individual insurers and infrastructure managers are not in a position to obtain and synthesize these data, since they span multiple companies and infrastructure authorities. The need for data is particularly critical in the realm of cyber risk.

A government-led data clearinghouse, similar to Verisk ISO products (verisk.com) could include a portal for insurers and infrastructure managers to share data on loss events and resiliency measures, which could then be used by many insurers and infrastructure managers in their decision-making. The development of publicly available loss models similar to those developed in the state of Florida for personal and commercial lines of residential property (http://fphlm.cs.fiu.edu/) or ongoing efforts such as the OASIS Loss Modeling Framework (oasislmf.org) would also be valuable.

Recommendation #4: Develop risk transfer/resilience metrics. These metrics would assist insurers with evaluating and comparing infrastructure systems and with implementing risk based pricing. They would also assist infrastructure managers in assessing their financial readiness to deal with a catastrophic disruption, and with evaluating and choosing resilience measures and insurance needs. One relevant example is the Los Angeles Metropolitan Transit Authority's Resiliency Indicator Framework (AECOM 2015). The indicators were developed to help them address climate change, including infrastructure resilience improvements and repairs.

Recommendation #5: Support research pertaining to emerging risks. Emerging risks are at the forefront of considerations for insurers and infrastructure risk managers. All those we interviewed mentioned emerging risks, with a focus on climate change, cyber, and terrorism-related risks. Uncertainty and data scarcity for these risks limit insurance and resilience measures. Support and facilitation of research to better understand and quantify these emerging risks is needed, along with the development of modeling tools for cyber risk.

Recommendation #6: Consider re-definition of terrorism for Terrorism Risk Insurance Act (TRIA) coverage. Infrastructure risk managers seem to opt out of TRIA coverage in some cases due to the restrictions on the coverage. TRIA coverage applies only to events that are officially deemed as terrorism events with losses of $140 million (in 2017), leaving many terrorism-like events uncovered. Trends in purchase of TRIA coverage should be analyzed to determine if purchase rates are declining. Broader coverage could be offered, or partnerships with private insurers to develop and promote products better suited to the needs to infrastructure entities addressing a range of terrorism-like events could be developed.

Recommendation #7: Highlight the comprehensive operational benefits to infrastructure managers of catastrophic risk insurance coverage beyond a straightforward loss backstop. Insurance provides financial security for infrastructure systems in light of disruptive and catastrophic events. Additional benefits associated with risk engineering and with risk and resilience financing have the potential to significantly impact the resilience of infrastructure systems in the United States. These benefits are not insignificant and should be recognized and advertised. Multi-year or dynamic insurance policies could result in closer risk management collaboration between insurers and infrastructure managers. More effort needs to be targeted at highlighting the business enablement value of insurance versus simply the price of the loss stop policy. Insurance empowers business by serving as a means of risk financing, enabling investment despite risk, while also serving as a barometer for risk. Infrastructure systems may also benefit from enhanced risk engineering and risk mitigation if the infrastructure-insurer relationship is viewed as a risk management partnership. Case studies of successful risk management partnerships between infrastructure and insurance could be developed to encourage more extensive insurance coverage.

Table 3 presents a cross-tabulation summary of the barriers to improving infrastructure resilience and insurance with recommendations for addressing each barrier. Future work should aim at understanding which of these barriers is most critical relative to the others in enhancing insurance penetration for critical infrastructure.

Future work will involve the development of infrastructure resilience metrics, with a focus on insurance and financial resilience to disruptions. These metrics will enable both infrastructure managers and insurers to assess infrastructure resilience and to track changes in resilience over time. Further research on the role that behavioral biases and moral hazard play in infrastructure resilience decisions will seek to address the behavioral barriers that limit the implementation of resilience measures and the purchase of sufficient insurance.

Table 3: Summary of barriers to infrastructure resilience and insurance and recommendations to address these barriers

Recommendations:	#1 Stafford Act revisions	#2 Alternative funding vehicles	#3 Data collection, availability and analysis	#4 Resilience Metrics	#5 Research on emerging risks	#6 Redefinition of terrorism for TRIA coverage	#7 Highlight benefits of catastrophic risk insurance
Infrastructure barriers:							
Funds to implement resilience improvements		X					
Data for risk assessment			X				
Evaluation and prioritization of resilience improvements			X	X			X
Protection from emerging risks			X		X	X	X
Insurance barriers:							
Data to support risk assessments for emerging risks			X		X		
Metrics to evaluate resilience improvements				X			
Demand for products	X	X					X
Ability to offer new products (real-time insurance, coverage for emerging risks)			X	X	X		

References

AECOM (2015). Resilience Indicator Framework for Los Angeles County Metropolitan Transportation Authority, December 2015, rev. 1. Accessed at: http://media.metro.net/projects_studies/sustainability/images/resiliency_indicator_framework.pdf

Amtrak (2015). Amtrak 2015 Sustainability Report.

ASCE (2017). American Society of Civil Engineers Infrastructure Report Card. Accessed at: http://www.infrastructurereportcard.org

Baylis, J., Gerstall, G.S., Scott, B., Grayson, M.E., Lau, C., Nicholson, J. (2015). Transportation Sector Resilience, Final Report and Recommendations. National Infrastructure Advisory Council, July 10, 2015.

Birkmann, J., Wenzel, F., Greiving, S., Garschagen, M., Vallée, D., Nowak, W., Welle, T., Fina, S., Goris, A., Rilling, B. and Fiedrich, F. (2016). Extreme Events, Critical Infrastructures, Human Vulnerability and Strategic Planning: Emerging Research Issues. *Journal of Extreme Events*, *3*(04), p.1650017.

Bonner, M. (2017). Do you Need Terrorism Insurance? *Business Insurance*. Accessed at: https://www.thebalance.com/do-you-need-terrorism-insurance-4102840

Burke, M., and Sipe, N. (2014). Urban Ferries and Catastrophic Floods: Experiences and Lessons Learned in Brisbane, Australia, and New York City. *Transportation Research Record: Journal of the Transportation Research Board*, (2459), 127-132.

Camillo, M. (2017). Cyber risk and the changing role of insurance. *Journal of Cyber Policy*, *2*(1), 53-63.

Chang, S. E. (2000). Disasters and transport systems: loss, recovery and competition at the Port of Kobe after the 1995 earthquake. *Journal of transport geography*, *8*(1), 53-65.

Chang, S. E. (2003). Transportation planning for disasters: an accessibility approach. *Environment and Planning A*, *35*(6), 1051-1072.

Chang, S. E., McDaniels, T., Fox, J., Dhariwal, R., and Longstaff, H. (2014). Toward Disaster-Resilient Cities: Characterizing Resilience of Infrastructure Systems with Expert Judgments. *Risk Analysis*, *34*(3), 416-434.

Establishing a Deductible for FEMA's Public Assistance Program (2017). FEMA supplemental advance notice of proposed rulemaking 82 Fed. Reg. 4064, January 12, 2017.

Kaddatz, M. M. (1995). *Risk Management for Small and Medium Transit Agencies* (No. 13). Transportation Research Board.

Kesan, J.P. and Hayes, C.M., Strengthening Cybersecurity with Cyber Insurance Markets and Better Risk Assessment (October 10, 2017). Minnesota Law Review, Forthcoming; University of Illinois College of Law Legal Studies Research Paper No. 17-18. Available at SSRN: https://ssrn.com/abstract=2924854

Kunreuther, H., and Michel-Kerjan, E. (2004). Dealing with extreme events: new challenges for terrorism risk coverage in the US. *Center for Risk Management and Decision Processes, Wharton School, University of Pennsylvania*.

Kunreuther, H., and Michel-Kerjan, E. (2011). *At War with the Weather: Managing Large-Scale Risks in a New Era of Catastrophes.* MIT Press. Paperback edition.

Kunreuther, H., and Michel-Kerjan, E. (2013). Managing the Risk of Catastrophes: Protecting Critical Infrastructure in Urban Areas. Presented to Federal Reserve Bank of New York, November 1, 2013.

Kunreuther, H., Michel-Kerjan, E., Lewis, C., Muir-Wood, R., and Woo, G. (2014). TRIA after 2014. *Wharton Risk Management Center, University of Pennsylvania*.

Kunreuther, H., Michel-Kerjan, E., and Tonn, G. (2016). Insurance, Economic Incentives and other Policy Tools for Strengthening Critical Infrastructure Resilience: 20 Proposals for Action. Wharton Risk Center paper.

Lazo, L. (2017). "Puerto Rico's roadways alone are a disaster, and it will cost at least $240 million to fix them. Washington Post, September 29, 2017.

Leavitt, W. M., and Kiefer, J. J. (2006). Infrastructure interdependency and the creation of a normal disaster: the case of Hurricane Katrina and the City of New Orleans. *Public works management & policy*, *10*(4), 306-314.

Litman, T. (2006). Lessons from Katrina and Rita: What major disasters can teach transportation planners. *Journal of Transportation Engineering*, *132*(1), 11-18.

Lloyd's (2017a). Managing the Escalating Risks of Natural Catastrophes in the United States. Accessed at: https://www.lloyds.com/news-and-insight/risk-insight/library/natural-environment/us-nat-cat-report

Lloyd's (2017b). Future Cities: Building Infrastructure Resilience. Accessed at: https://www.lloyds.com/news-and-insight/risk-insight/library/society-and-security/arup

Meade, C., and Kulick, J. (2007). *SB1953 and the challenge of hospital seismic safety in California*. Oakland: California HealthCare Foundation.

Ng (2017). How risk modeling propels the cyber insurance market forward. Property Casualty 360.

Ortiz, D. S., Ecola, L., and Willis, H. H. (2009). Freight Transportation Resilience: How a System-Wide Perspective Can Help Metropolitan Planning Organizations and Departments of Transportation. NCHRP Project 8-36.

Rakich, R., Wells, C., and Wood, D. (2011). *Airport Insurance Coverage and Risk Management Practices* (No. Project 11-03, Topic S01-03).

Renn, O. (2014). Emerging risks: Methodology, classification and policy implications. *Journal of Risk Analysis and Crisis Response*, *4*(3), 114-132.

Schwab, M., Berchtold, C., and Goris, A. (2016). An Integrated Critical Infrastructure Risk and Resilience Concept in the Context of Extreme Weather Events and Global Change. *Journal of Extreme Events*, *3*(04), 1650015.

Travelers Risk Index (2016). Accessed at https://www.travelers.com/resources/risk-index/2016-business-industry-charts.aspx

U.S. Department of Energy. (2013). Insurance as a Risk Management Instrument for Energy Infrastructure Security and Resilience.

Vajjhala, S., and Rhodes, J. (2015). Leveraging Catastrophe Bonds as a Mechanism for Resilient Infrastructure Project Finance. REbound.

Wilbanks T, Fernandez S, Backus G, Garcia P, Jonietz K, Kirshen P, Savonis M, Solecki W, Toole L, and Allen M. (2012). Climate change and infrastructure, urban systems and vulnerabilities. Technical Report for the US Department of Energy in Support of the National Climate Assessment.

Woods, D., and Simpson, A. (2017). Policy measures and cyber insurance: a framework. *Journal of Cyber Policy*, *2*(2), 209-226.

Appendix A: Interview questions for Insurers and Infrastructure Managers

<u>Interview Questions for Insurers</u>

Current offerings

1. Describe the types of transportation systems that your company currently does business with (length of involvement, successes, issues).

2. Do you insure against all types of infrastructure disruptions including natural hazards, manmade hazards (i.e. terrorism and cyber threats), accidents, and infrastructure failures? Do transportation entities purchase different policies for different hazards (e.g. flood, terrorism)?

3. What types of insurance products do you offer that are relevant to transportation infrastructure systems? Do these products link with any other resilience enhancing activities (i.e. mitigation)? How do your products address interdependencies in the system? Or how do they address geographic concentration of risk? Do your products only deal with direct property losses or indirect losses to the business?

4. Describe one of your relevant policies. Did you place this policy yourself, or are you working with a broker?

5. With whom do you interact on the policy coverage (risk management personnel, other)? How often do you interact with them? Do you or the infrastructure firm actively manage their risk and is your product tailored to this risk? How is the risk of the infrastructure system analyzed, and by whom? Do they use an insurance broker? Are the clients savvy risk consumers?

6. What has been the most significant risk dealt with under the policy?

7. Which layers of risk transfer do your transportation clients employ? (Self insurance: mitigation measures, budgeting/saving for disruptive events; Insurance; Reinsurance; Government assistance) How are these risk transfer practices taken into consideration when setting the terms of a policy?

8. What is the role of reinsurance or other alternative risk instruments in offsetting your risk in insuring them?

9. Has your insurance program changed as a result of Superstorm Sandy that hit the NY/NJ area in October 2012? If so, in what ways (e.g., lower or higher deductibles or coverage limit, higher costs per dollar of coverage, lack of availability of coverage?)

10. Has your insurance program changed as a result of any other natural or man-made damaging events? (e.g., lower or higher deductibles or coverage limit, higher costs per dollar of coverage, lack of availability of coverage)

11. What is the process to measure risks due to cyber threats caused by exploitation of known

vulnerabilities in any specific technology or web-based communication?

12. Is there a good understanding of the impacts of cyber attacks on transportation infrastructure (operation/services delay, passenger injury, damages to freight, data theft)?

13. Does cyber risk management in transportation systems follow guidelines such as, NIST Risk Management Framework, ISA/IEC/ISO Standards, ICS-CERT recommendations?

14. Are there differentiated insurance policies for organizations that use archaic or outdated systems that are more vulnerable to exploitation?

15. What are the processes to ensure that organizations can identify if subsequent cyber attacks are similar to prior attacks? Are there incentives for organizations that implement changes to address known threat and ensure the same vulnerabilities are not exploited again?

Barriers to catastrophe insurance for transportation infrastructure

16. Broadly, transportation infrastructure includes aviation, roads and bridges, inland waterways, ports, rail, and transit. Describe (size, number of insurers, regulatory setting, private vs. public client base, profitability) the transportation insurance marketplace as a whole or any of the particular components. How has it changed over time, or how do you see it changing? What role does the quality and age of infrastructure play?

17. Is there any coverage that is currently not included in your policies, but you would like to provide in the future? What do you see as the major obstacle to providing this coverage?

18. What do you see as key barriers to enhancing the robustness of risk transfer for transportation infrastructure systems? Do you see more barriers on the supply or demand side?

19. Explain the role of quantifying the risk (how good is the modeling), profitability, premium setting, adverse selection, moral hazard, correlated risk, rating agencies. Where do you get your data?

20. What do you see as key barriers to improving resilience in the transportation infrastructure systems?
    a. Do you see regulations as barriers?
    b. Do you see finances as barriers?
    c. Do you see other barriers?

21. How does the state of infrastructure repair impact insurance?

22. There are known behavioral concerns regarding decision-making for low probability/high consequence events (availability bias, threshold models, imperfect information, myopia).

Do you observe these with your clients? Are there other behavioral concerns with regards to your clients' risk management?

23. When evaluating risks and setting the terms of the policy, are the cybersecurity practices of transportation entities more or less important than the cybersecurity practices of policy holders in other sectors?

<u>Interview questions for transportation infrastructure managers</u>

Insurance and Risk Transfer Decisions

1. Do you purchase insurance to cover losses from natural and man-made disasters? If "yes," what is the deductible and coverage limit? Can you provide details or an example of one of your policies?

2. Do you buy insurance from a single company or from multiple insurers in a dedicated insurance program placed for you by an insurance broker? Explain why.

3. Do you have sufficient funds for maintenance? Do you need to choose between spending for maintenance or insurance? Or maintenance or resilience improvement?

4. Do you have any interactions with the community in your insurance or risk management decisions?

5. Are you aware of the $200 million catastrophe bond issued by the New York's MTA issued after Superstorm Sandy? Have you considered issuing such a cat bond?

6. Has your insurance program changed as a result of Superstorm Sandy that hit the NY/NJ area in October 2012? If so, in what ways (e.g., lower or higher deductibles or coverage limit, higher costs per dollar of coverage, lack of availability of coverage)

7. Has your insurance program changed as a result of any other natural or man-made damaging events? (e.g., lower or higher deductibles or coverage limit, higher costs per dollar of coverage, lack of availability of coverage)

8. Are you self-insured for all types of losses related to natural and man-made disasters? If "yes," do you have a captive? If self-insurance is partial, how much self-insurance do you have?

9. In a worst-case scenario, how much do you estimate natural and man-made disasters would cost your company after taking into account your insurance and self-insurance provisions?

10. Do you feel comfortable that your current insurance/financial strategy is adequate to handle such a loss?

11. Do you rely on reinsurance or government assistance as part of your risk management strategy?

12. What do you see as key barriers to enhancing the robustness of risk transfer for transportation infrastructure systems? Do you see more barriers on the supply or demand side?

Post-Disaster Recovery

13. Have you ever received any government post-disaster funding? If Yes, after which disaster?

14. How much public funding did you receive and for what purposes? How long did it take your organization to receive these funds?

15. How much of the post-disaster cost was covered by insurance? How long did it take your organization to get these insurance payments?

16. How much did you have to cover from your own surplus?

17. Do you expect to receive any government post-disaster funding should you experience a severe disaster in the next 5 years?

Measures to Reduce Future Losses

18. What actions have you taken to reduce potential losses and facilitate your recovery from natural and man-made disasters or other severe disruptions? (self-insurance, insurance, reinsurance, government assistance)

19. What actions are you planning to take in the future to reduce potential losses and facilitate your recovery from natural and man-made disasters or other severe disruptions?

20. Have you estimated your probable maximum loss resulting from these events? If yes, how much is it? If yes, have you estimated the likelihood of such an event occurring in a given year?

21. What is your current financial protection and recovery strategy to deal with natural and man-made disasters or other severe disruptions? Has it been discussed with the CEO and Board of Directors? When?

View of the risk

22. How does your firm approach/manage the four main types of infrastructure disruptions including natural hazards, manmade hazards (i.e. terrorism and cyber threats), accidents, and infrastructure failures?

23. How effective do you find this approach?

24. What experiences have you had (or almost had) in regard to any of these main risks? How big have the losses been? Were these direct or indirect losses?

25. How do your peers view these risks?

26. What is your view of infrastructure resiliency – what does this mean to you?

27. What, if any, is the current role of network security in your resilience plans?