Cyber Risk and Insurance for Transportation Infrastructure

Gina Tonn (gtonn@wharton.upenn.edu)
Risk Management and Decision Processes Center,
Wharton School, University of Pennsylvania

Jay Kesan
University of Illinois

Jeff Czajkowski
Risk Management and Decision Processes Center,
Wharton School, University of Pennsylvania

Linfeng Zhang
University of Illinois

March 2018
Working Paper # 2018-02

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/

.

Cyber Risk and Insurance for Transportation Infrastructure

Gina Tonn[a], Jay P. Kesan[b], Jeff Czajkowski[c], and Linfeng Zhang[d]

a. Corresponding author. Wharton Risk Management and Decision Processes Center, University of Pennsylvania, 3819 Chestnut Street, Suite 130, Philadelphia, PA 19104, USA; phone: 1-215-746-0473; fax: 215-898-5688; email: gtonn@wharton.upenn.edu
b. University of Illinois, 504 East Pennsylvania Avenue, Champaign, IL 61820, USA; email: kesan@illinois.edu
c. Wharton Risk Management and Decision Processes Center, University of Pennsylvania, 3819 Chestnut Street, Suite 130, Philadelphia, PA 19104, USA; email: jczaj@wharton.upenn.edu
d. University of Illinois, 504 East Pennsylvania Avenue, Champaign, IL 61820, USA; email: lzhang18@illinois.edu

Abstract

While advances in information technology and interconnectivity has improved efficiency for transportation infrastructure, they have also created increased risk associated with cyber systems. This study includes both an analysis of cyber incident data for transportation systems and a series of interviews with transportation infrastructure managers and insurers. The objective is to identify barriers to a robust cyber insurance market and improved cyber resilience for transportation infrastructure. Results indicate that the annual number of cyber incidents and associated costs are on the rise. The most common incidents involve data breach, while incidents involving unintentional data disclosure have the highest average loss per incident. Cyber risk assessment, mitigation measures, and insurance are being implemented to varying degrees in transportation infrastructure systems, but are generally lacking. Infrastructure managers do not currently have the tools to rigorously assess and manage cyber risk. Limited data and models also inhibit the accurate modeling of cyber risk for insurance purposes. Even after improved tools and modeling are developed, residual cyber risk will be significant, and insurance purchase is an important risk management strategy to allow transportation infrastructure systems to recover from cyber events.

Keywords: transportation; cyber risk; cyber insurance

1 Introduction

Transportation systems support the movement of people and goods within a defined region and include the combination of vehicles, infrastructure, and operations that enable these movements [1]. The U.S. transportation network includes aviation, roads and bridges, inland waterways, ports, rail, and transit. These transportation systems are vital to the U.S. economy and way of life, and disruptions can have short-term and long-term socio-economic impacts.

Information technology and interconnectivity have improved efficiency and functionality for transportation infrastructure. However, they have also brought increased risk associated with cyber systems that are now essential for safe and continuous operation of transportation systems [2]. According to the US Department of Homeland Security, there are more than 60 US critical infrastructure entities for which damage associated with a single cyber entity could potentially result in $50 billion in economic damages, 2,500 immediate deaths, or a severe impact to US national defense [3]. Cyber risks are increasing, and cyber related losses are growing as new technologies are implemented and reliance on them increases. Thus, it is likely that full cybersecurity for transportation infrastructure is not achievable solely by technological improvements. Therefore, in addition to attempting to prevent attacks and lower cyber risk, transportation managers should also prepare financially for inevitable losses through self-insurance and insurance [4]. Cyber insurance is currently available, but limited, and expansion of cyber insurance coverage is needed to manage the growing risk.

In this study, we aim to identify barriers and opportunities for a robust cyber insurance market and improved cyber resilience for transportation infrastructure. Section 2 provides background on general cyber risk and insurance as well as cyber risk specific for transportation infrastructure. Section 3 describes methods and data. Section 4 provides insights from analysis of cyber incident data for transportation systems. Section 5 describes the current state of cyber insurance for transportation infrastructure based on the findings from interviews with insurers and infrastructure managers. Section 6 concludes and presents recommendations for future research.

2 Background

2.1 Overview of general cyber risk and insurance

Cyber losses can be associated with liability from a customer data breach, property damage and theft (e.g., accidents caused by compromise of signaling systems), data damage (e.g., hacking maritime cargo management systems), loss of income due to outages and failure, website defacement, and cyber extortion [5]. Cyber attackers can be hackers, criminal organizations and thieves, state-sponsored attackers and spies, other companies or organizations, terrorists, malicious insiders, and contractors [6,7]. There are four main layers of cyber systems, each of which are at risk for cyber attack. The first is the perceptual layer, which links cyber and physical through components like wireless sensors and GPS. The second is network systems which transmit information (e.g. satellite networks and the internet mobile communication network).

The third is support systems such as cloud computing and intelligent computing, and the fourth is the application layer which links users and the physical world with cyber systems (e.g. intelligent transportation and environmental monitoring [8].

Given the variety of possible cyber losses, there are also a variety of approaches to mitigating these losses which can include design methods which improve system architecture and activities, or operational methods that involve changes to business operations [8,9]. Other approaches to managing cyber risk include countermeasures like security software, system design and operations improvements, and investments in the cyber workforce. Protective measures like firewalls, software encryption, virus detection, and system compartmentalization are also used to reduce cyber risk. Security benefits of these protective measures must be balanced against associated costs and productivity losses. Institutional measures for managing cyber risk can be structural (software and hardware), procedural (management and operation of systems), and responsive (response and damage management after an incident is detected) [6].

2017 was possibly the worst year for cyber attacks to date, with three significant events changing the cyber risk landscape. In May 2017, the WannaCry ransomware attack created global impacts including significant effects on the UK Health System. In June 2017, the NotPetya virus was launched in Ukraine and spread to many parts of the world, resulting in over $1 billion in economic damage. In August 2017, a breach at the Equifax consumer credit agency created a market cap loss exceeding $5 billion [10]. Marsh & McLennan predicts the situation to worsen and identified two emerging trends. The first is attacks on industrial control systems, with the potential for cyber attacks to result in physical damage. The second is a tightening of cyber security laws as attacks grow more severe.

The extensive nature of cyber attacks in 2017 highlights that sufficient cyber risk management cannot be achieved solely through information technology management that attempts to mitigate the risk. A further way to deal with the residual cyber risk is to transfer the risk through insurance. And as cyber risks increase, heightened concern among executives over liability associated with customer data breach as well as financial and operational effects of cyber risks will likely drive changes in cyber insurance purchases and in the cyber insurance market with policies that reflect the expanding nature of cyber attacks. For example, on the demand side, businesses will likely turn to more tailored enterprise cyber insurance policies, whereas on the supply side insurers will likely limit the cyber loss coverage of traditional property, casualty, and other business policies [11].

Existing cyber risk insurance coverage generally includes liability, remediation, and legal and regulatory fines and penalties and is primarily designed to cover losses associated with a data breach. New or future products could address more holistic coverage for operations, system failures, business interruption, and supply chain disruption [5,12]. And even today, cyber policies are generally very client-specific and negotiated on a case-by-case basis. In addition to the transfer of risk to willing partners, benefits of cyber insurance include incentivization of investment in IT security, and a boost in overall IT security, because as cyber insurance increases, best practices and standards spread through the economy [4,13]. Accordingly, the cyber

insurance market is growing in the U.S. in conjunction with the rising number and cost of data breaches. As of 2015, the U.S. cyber insurance market had $2-$2.5 billion of gross written premium. However, 40% of companies surveyed by insurance broker Aon did not assess cyber risk or assessed only by "gut feel" [12]. Unlike terrorism risk, cyber risk has the potential for a thorough data set to support a robust insurance market.

However, the cyber insurance market is relatively new and not yet mature. How to set premiums is a key question for the development of a more mature cyber insurance market. Setting premiums is particularly challenging due to lack of actuarial data from past events and lack of normative standards [4]. Some cyber risks may not be quantifiable, and therefore are not insurable. The ability to model cyber risk is currently limited, but will improve substantially as more data is accumulated and shared. Additionally, cyber insurance products lack clear loss triggers and objective determination of loss severity [12].

Beyond the issues surrounding the quantification of risk, conceptual issues exist around correlated risk and lack of re-insurance. Also, traditional insurance market issues apply to cyber insurance, including moral hazard and adverse selection caused by information asymmetry. For example, there is a moral hazard associated with companies that may not feel the need to improve cyber security if they are insured [4]. Other cyber insurance challenges include a lack of legal framework, with uncertainty in liability and lack of cyber standards. All-told, cyber insurance hasn't fully taken off yet due to these issues, and market inexperience leads to conservative pricing [5]. However, Aon estimates that by 2025, cyber will be a major line of business for insurers [12].

2.2 Cyber risks for transportation infrastructure

The various modes of the U.S. transportation system act as a system of systems locally, regionally, and nationally. Transportation infrastructure consists of three main components: hard infrastructure, vehicles, and operations components. Network infrastructure and components are a key part of the hard infrastructure [8].

In this study, we are focused on three primary types of transportation infrastructure: aviation, rail and transit, and marine. U.S. aviation infrastructure includes aircraft, air traffic control systems, about 450 commercial airports, and 19,000 additional air transportation facilities for movement of people and cargo [14]. Rail and transit systems operate locally and nationally, and include a variety of modes of transportation including trains, buses, subways, trolleys, and the systems that support passenger and cargo transport. U.S. freight rail includes over 140,000 miles of active railroad and 1.3 million freight cars, with over 12,000 trains operating daily [14]. Marine transportation includes cargo transport and cruise ship passenger transport. Components include ports, ships, and control systems. IT systems are used to manage the movement of vehicles and to control vehicular traffic. They are also vital to the management, identification, and tracking of passengers and cargo throughout the system.

Transportation infrastructure is subject to cyber dependency, where its state is dependent on information transmitted through information infrastructure. This information infrastructure is used to manage the flow of vehicles and goods, and the reliance on information technology and communications infrastructure makes transportation infrastructure particularly susceptible to cyber-attacks [15,16]. Cyber-attacks can affect the power grid, sea port operations, air traffic control, and other components and services of transportation infrastructure. A cyber-attack on global positioning systems could significantly impact many infrastructure sectors, including transportation infrastructure [6].

Cyber risk is significant and growing in the aviation industry, with 85% of airline CEOs expressing concern about cyber risk. Airlines are at risk for theft of customer or company data, but also for their communications and connectivity systems to be compromised. Managing aviation cyber risk requires efforts from airlines, manufacturers, maintenance providers, air traffic controllers, airports, and third-party suppliers. Cybersecurity measures can include threat intelligence, identity and access management, data protection and encryption, application security, and security awareness [17].

Cyber systems are used in rail transport for communications-based automatic train control. Cyber components include wireless communication and control systems, both of which can be subject to cyber-attacks [18]. Cybersecurity measures are needed to reduce the risk of data loss and to ensure steady and stable rail operations. Previous rail related cyber incidents include a 2008 derailment of tram trains in Poland via an adapted TV remote, a two-day shutdown of train service in the northwest U.S. in 2011 due to remote computer attacks, and a 2016 ransomware attack on the San Francisco Bay Area Rapid Transit (BART) ticketing machines which disrupted public transit [19].

Cyber incidents impacting marine transportation can involve navigation, cargo control, and other industrial processes, threatening lives, the environment, and property, and disrupting trade activity. Marine cyber disruptions can impact control of temperature for refrigerated containers and emergency systems. Port operations such as raising a drawbridge, controlling traffic lights, scheduling trucks, and controlling pumps, values, and pipelines for delivery of fuel and liquid cargo to ships can be impacted. There are two factors increasing marine cyber risk: increasing control of computer systems and increasing networking of computers with each other and the internet. One example of a cyber-marine incident involved malware impacting a dynamic positioning system used in the offshore oil industry for precise navigation control. Malware on a crew member's smart-phone which was plugged into an electronic chart system deleted or corrupted all charts, causing a two-day delay. In another incident, organized crime exploited a European container terminal's tracking system for cargo, allow for use of the system in drug smuggling [7].

3 Methods and Data

3.1 Cyber incident data and analysis methods

One approach we use to understand and get more insights into the cyber risk in the transportation infrastructure industry is to study the historical cyber incidents collectively. The incident data is provided by Advisen, a leading data provider in the property-and-casualty insurance market. Unlike many other data sources, which are mostly voluntary reporting databases, such as VERIS Community Database (VCDB: http://vcdb.org) and Web Hacking Incident Database (WHID: http://projects.webappsec.org/w/page/13246995/Web-Hacking-Incident-Database), Advisen is actively collecting cyber incidents from various information channels, and maintaining and updating the database periodically, so it has advantages over other databases in terms of the quality and quantity of information, which help us deliver more accurate results.

In the database, currently over 40,000 cyber incidents are recorded, and each record comprehensively covers the most important aspects of an incident, including:

- Information about the victim company
- Case characteristics including affected asset, case type, etc.
- A timeline marking different stages during the development of this incident
- Outcomes including loss types and loss amounts

With the victim company information, we can tell the industry that each company operates in by its NAICS (North American Industry Classification System) code. To match the scope of this study, which primarily consists of aviation, rail and transit, and marine transportation infrastructures, we distinguish companies in transportation infrastructure industry from companies in other industries, and we define transportation infrastructure industry as a collection of sub-industries based on their 6-digit NAICS codes.

Then, to study the cyber risk in transportation infrastructure industry, we define cyber risk as the potential occurrence of incidents with information systems involved, and the incidents can originate from various types of causes. In this study, we consider not only risks associated with potential malicious actions, such as hacking or phishing, but also risks arising from data handling procedures, such as the privacy violation during data collecting or disclosing process. Table 1 describes the cyber incident types included in our analysis.

Table 1: Cyber Incident Types

Privacy Violation	Privacy - Unauthorized Contact or Disclosure Privacy - Unauthorized Data Collection
Cyber disruptions that affect business operations	Denial of Service (DDOS)/System Disruption Network/Website Disruption Industrial Controls & Operations
Unauthorized access to information systems for financial gain	Cyber Extortion Digital Breach/Identity Theft Identity - Fraudulent Use/Account Access Phishing, Spoofing, Social Engineering Skimming, Physical Tampering
Malicious data breach and IT failures	Data - Malicious Breach Data - Physically Lost or Stolen IT - Configuration/Implementation Errors IT - Processing Errors
Unintentional data disclosure	Data - Unintentional Disclosure

We acquire additional data from the US Census Bureau to provide some background information on the industry, and along with the cyber incident data, we study the cyber risk within the transportation infrastructure industry by recognizing major trends in cyber incidents in terms of frequency and severity and identifying the key threats to this industry.

3.2 Interviews with transportation infrastructure managers and insurers

Interviews and discussions were undertaken with insurers and infrastructure managers as well as with researchers having expertise in resilience of air transport infrastructure and cyber resilience for infrastructure systems. The purpose of the insurer interviews was to gain insight from insurers on current cyber insurance offerings along with barriers to expanded offerings and hindrances to cyber insurance demand. Interviews with infrastructure managers were undertaken to gain insight into current cyber risk management tactics, cyber risk perception, and insurance uptake in transportation infrastructure systems. Table 2 describes the roles and transportation focus areas of the interviewees.

Table 2: Summary of Interviewees

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

While the interviews focused broadly on risk and insurance for transportation infrastructure systems, cyber risk and insurance were included in each discussion. Topics of discussion included specific concerns about cyber risk, modeling and management of cyber risk, and cyber insurance. Insurers discussed their current cyber insurance offerings and research needs to enable a more robust cyber insurance market. Infrastructure managers discussed their perceptions of cyber risks as they pertain to their infrastructure system, cyber risk mitigation measures, and if or how their system is insured against cyber risks. Both insurers and infrastructure managers suggested research needs and other advances that they expect would enhance infrastructure cyber resilience and insurance.

4 Analysis of cyber incident data for transportation infrastructure

As discussed in Section 2.1, risk assessment data is a key limitation to the current state of cyber insurance for transportation infrastructure. However, some data on transportation-related cyber incidents is available, and we analyzed it to gain a better understanding of the number and types of transportation related cyber incidents, as well as the costs of these incidents.

By selecting the cyber incidents in the transportation infrastructure industry as previously defined, we obtain 284 records from the database[1]. This number possibly underestimates the true number of occurrence, because only a portion of all the cyber incidents are reported and recorded [20]. Security breach notification laws enacted in many states in the early 2000s help mitigate the problem by requiring organizations to disclose data breach incidents with customer information involved. So, in regard to the incident number and frequency, we primarily look at the 214 incidents taking place between years 2006 and 2015, which provide us a more accurate estimate of the true trend of cyber risk in this industry. Figure 1 illustrates the number of incidents per year, the number of affected companies, and the number of incidents per company over this period.

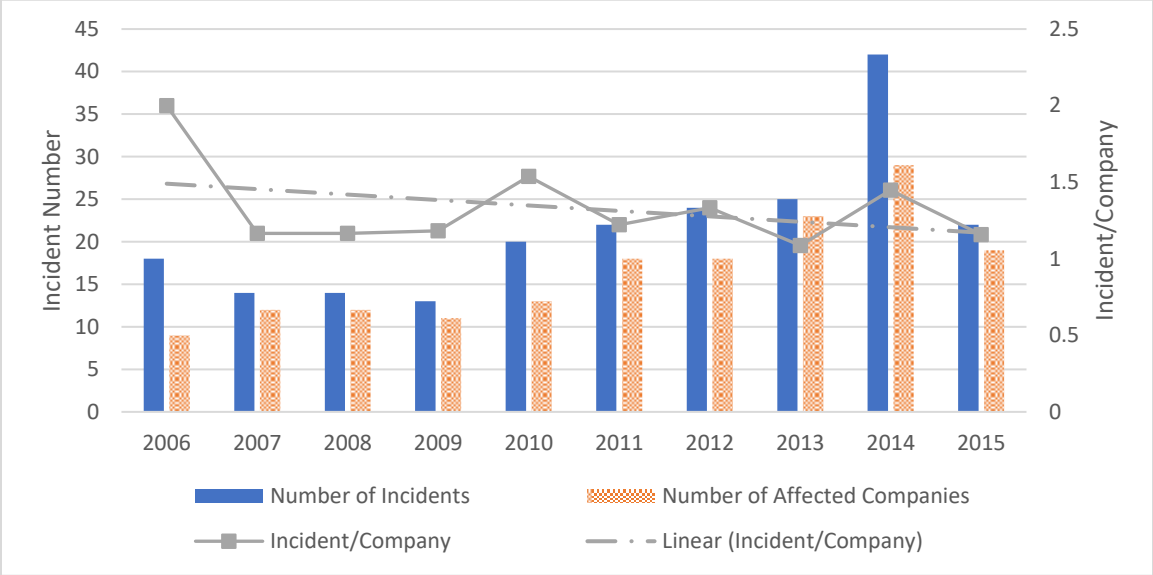

Figure 1: Cyber Incident Numbers

From 2006 to 2015, both the incident numbers and numbers of affected companies in the transportation infrastructure industry are growing. To see if such growth in number of affected companies is driven by the increase in number of companies in this industry, so that the likelihood of a company experiencing at least one cyber incident in a year roughly remains the same, we have examined SUSB (Statistics of U.S. Businesses) Annual Datasets in year 2007 and 2012 from US Census Bureau. From the datasets, we find that the total number of companies in the transportation infrastructure industry has declined from 158,888 in 2007 to 152,963 in 2012 at an average rate of -0.76% per year, while the annual number of companies affected by cyber incidents has experienced a 50% growth from 12 to 18 during this period. If we assume the declination rate in number of companies in the transportation infrastructure industry to be

[1] With respect to the number of cyber incidents, the Transportation and Warehousing sector is ranked 13th among all the 20 NAICS sectors, thus representing a relatively small group. The top 4 sectors are Finance, Healthcare, Public Administration and Information, which are of greater interest to cyber criminals and contribute more than half of the incidents in the entire dataset.

constant, then the growth in number of affected companies over the past years is truly driven by the spread of cyber risk. This suggests that companies in this industry are more likely to be hit by cyber incidents nowadays than in the past. In spite of such spread of cyber risk within the entire industry, we notice that individual companies are getting less hit by cyber incidents, because the incident/company ratio is decreasing over the past years indicating that it is becoming less likely for individual companies to repeatedly experience cyber incidents. Both the increase in number of incidents in the industry and the decrease in number of incidents experienced by individual companies suggest a trend that cyber risk is becoming more commonplace in the transportation infrastructure industry, and thus many companies which have never had cyber incidents in the past should get prepared for possible future incidents.

20 out of the 214 incidents have known loss information. As shown on Figure 2, the loss distribution suggests that 20% (4/20) of the incidents in the transportation infrastructure industry did not result in any actual losses, and most of the losses were within the $0.1 million to $10 million range.

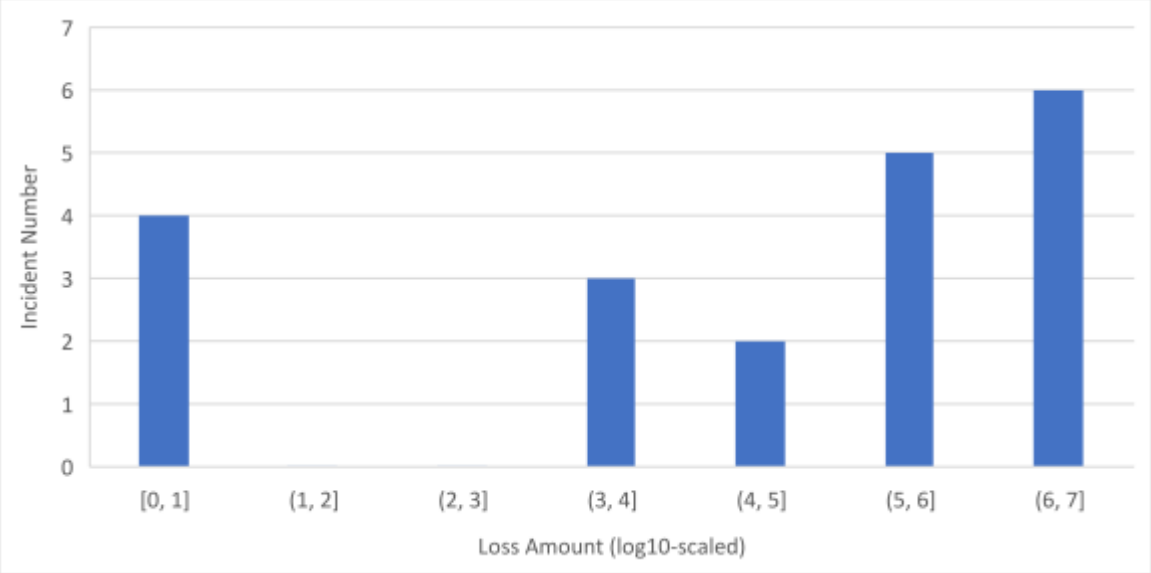

Figure 2: Cyber Incident Losses Distribution

By looking at how the loss amount evolves over time (Figure 3), we find that the yearly average loss resulting from a single cyber incident in this industry is typically around $1 million and is slowly getting higher in recent years. The maximum of losses caused by a single incident keeps increasing over time at a much faster pace, which means that although most of the losses are still quite small, in the case of extreme events, the losses suffered by victim companies are becoming more unbearable. If such situation continues, companies will have to consider transferring some of the risk to other parties since retaining the risk is getting costlier and less efficient, and one way of doing so is through cyber insurance. So, we expect to see an increase in demand for cyber insurance in the transportation infrastructure industry.

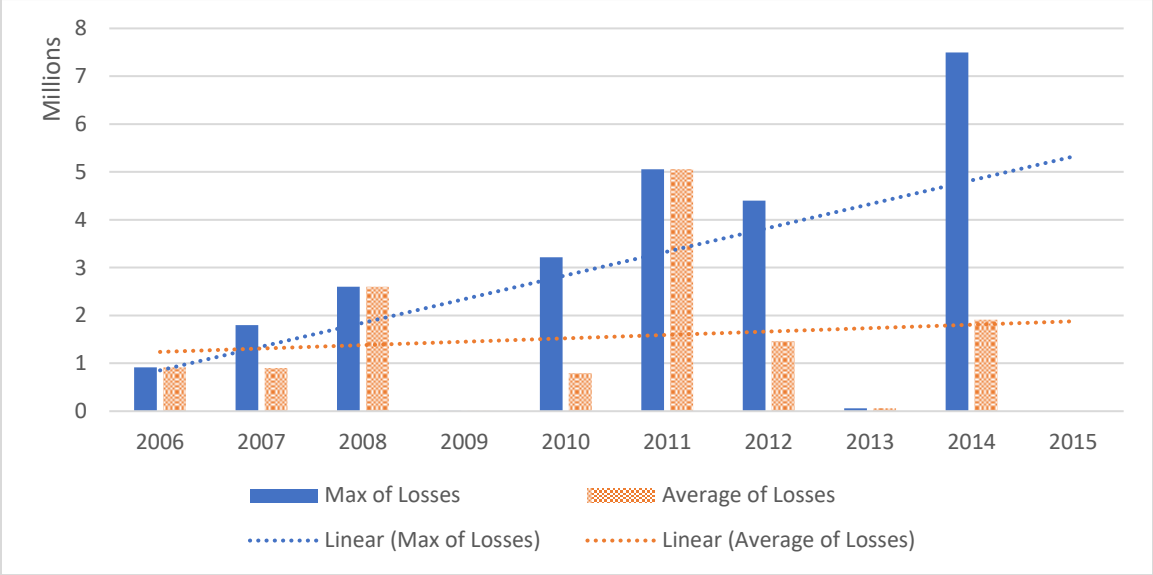

Figure 3: Cyber Incident Losses by Year

Cyber risk can lead to a variety of incident types, as illustrated on Figure 4. In the transportation infrastructure industry, the most common incident type is malicious data breach, which is the leak of confidential information caused by malicious actors. Malicious data breaches make up 27.1% (58/214) of all incidents, and they result in an average loss of $0.33 million. Privacy-related incidents also have a very high occurrence frequency. Unauthorized Contact or Disclosure and Unauthorized Data Collection together account for 22.9% (49/214) of the incidents, and the average losses are respectively $1.52 million and $1.61 million, which are more severe than the losses caused by malicious data breaches. Among all the incident types, unintentional disclosure of data has the most destructive impacts on victim companies with an average loss of $3.17 million. Incidents in this category typically result from a company failing to comply with information disclosure regulations. For example, the costliest cyber incident in this industry was caused by an airline company disclosing customers' credit card information on receipts in an inappropriate way that violated the Fair and Accurate Credit Transactions Act (FACTA) amendment to the Fair Credit Reporting Act (FCRA). This incident cost the company $7.5 million to settle the complaint [21].

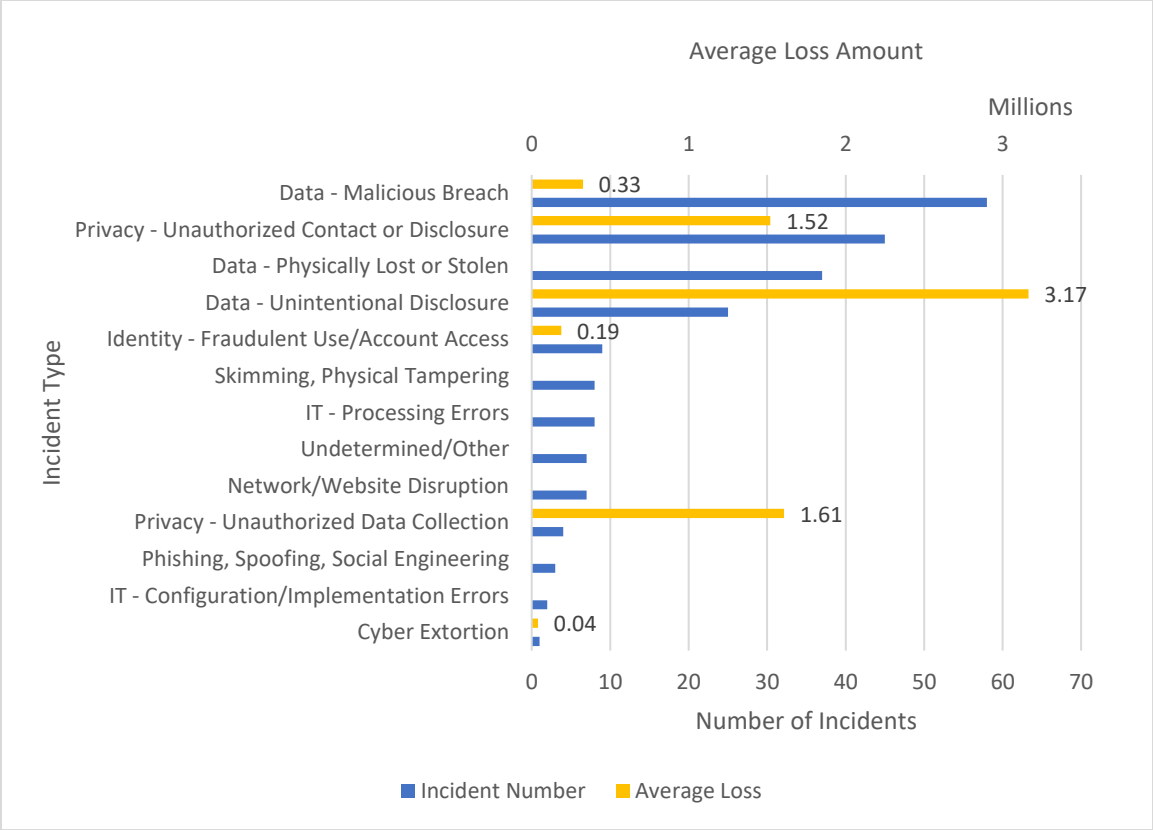

Figure 4: Frequency and Severity by Incident Type

The analyses on historical data, albeit a relatively limited set of data, suggest that both the frequency and the severity of cyber incidents are on the rise. The landscape of cyber risk in the transportation infrastructure industry is fast changing, thus making the environment more challenging for risk managers.

5 Cyber risk, perception, and insurance for transportation infrastructure

In the interviews, infrastructure managers expressed concern about cyber risk, and called out concerns about the uncertainty in the risk and the unknown component of the risk. Insurers are offering cyber insurance products, but noted that there are constraints on policy limits associated with the emerging and unknown nature of the risk. Models are in development to simulate and estimate cyber risk and potential damage, but until models are further developed, insurance is market-priced, and limits are constrained. Because cyber risk is still considered new and poorly understood, infrastructure managers desire 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.

At least 20 insurers currently sell cyber insurance, offering first-party coverage for losses directly incurred and third-party coverage for liabilities of others and for issues such as damage to others'

IT systems and fines associated with data breaches of personal information. Just as insurance has played a role in the development of standards and codes for other insured risks (e.g. fire), insurers could promote standards and information sharing for cyber risk [22].

Three infrastructure managers interviewed indicated that their systems are covered for cyber risk and one noted that they do not have cyber coverage. The three that had coverage noted that coverage is limited, and that they feel that available models of cyber risk are inaccurate. The infrastructure manager for the system that does not have coverage is currently assessing the need for cyber insurance.

Insurers noted a number of concerns as they work to develop models of cyber risk and to broaden their cyber insurance offerings. These concerns include a lack of data that inhibits risk-based pricing, insufficient mitigation of risk by clients who hope that the government will address concerns outside of their reach, and the challenge of building a balanced portfolio in the area of cyber insurance. There are no geographical boundaries to cyber risk, so a single cyber event could have global impacts. A key challenge for cyber insurers is building up a diversified set of cyber insurance clients to provide a balanced portfolio of risks that are not highly correlated with respect to future disruptions. This balanced portfolio of risk is needed to position cyber risk as an insurable risk [23]. 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.

Both insurers and infrastructure managers that were interviewed expressed the need for improvements in the modeling of cyber risks. Data collection, sharing, and availability were noted as important components of modeling cyber risk. Due to the emerging nature of the risk, data is limited, and this hinders effective modeling of the risk. Lack of data sharing amongst utilities and insurers further compounds the issue of accumulating sufficient data to effectively model transportation cyber risk. In addition to the need for models and data, metrics are needed so that cyber risk can be effectively quantified and measured, and so that benefits of cyber risk reduction measures can be quantified.

One insurer indicated that they are undertaking vulnerability modeling for cyber risk and are developing a plan with infrastructure managers for managing this risk. This insurer indicated that there tend to be many relatively easy or inexpensive improvements in cyber security that infrastructure managers can be made aware of in the short term before addressing issues that require complex models. As both infrastructure managers and insurers work to better understand and model cyber risk, these simpler improvements in cyber security can lower risk while more comprehensive measures are identified and evaluated.

As is prevalent with other types of risks, infrastructure managers interviewed exhibited differing perceptions and somewhat biased views of cyber risk. Understanding and addressing these varied perceptions and views is needed to encourage a robust cyber insurance market. A study by deSmidt and Botzen found that awareness about cyber risk and perceived probability of cyber incidents are high, but expected impacts of a cyber incident are often underestimated [3]. This

potentially impacts the uptake of cyber insurance. Further study on the role of behavioral biases in the management of cyber risk, including the purchase of cyber insurance, is needed along with advancements in modeling, data, and metrics in order to facilitate a robust cyber insurance market for infrastructure systems.

In Section 2.1, we highlighted a number of issues noted in the literature related to the difficulties of establishing a robust insurance market for cyber insurance. Our interviews provided further insight into these issues for the transportation infrastructure sector. Infrastructure managers noted that available cyber insurance coverage tends to be limited in scope and not as broad as the managers would like. Both insurers and infrastructure managers highlighted the challenges in modeling cyber risk including limitations in data availability and modeling methods. These challenges lead to difficulty for insurers in setting risk-based premiums. While those interviewed did not specifically discuss moral hazard and adverse selection issues, addressing those issues along with risk perception and behavioral biases are crucial in developing a robust cyber insurance market for transportation infrastructure.

6 Conclusions and Research Needs

Air, rail, transit, and marine transportation infrastructure systems are all subject to a variety of cyber risks that have the potential to impact system operations and data privacy. Cyber incidents cause disruptions to transportation infrastructure systems and threaten the security of system and customer data. A review of transportation related cyber incident data indicates that the annual number of cyber incidents and associated costs are on the rise. The most common incidents involve data breach, while incidents involving unintentional data disclosure have the highest average loss per incident.

Cyber risk assessment, mitigation measures, and insurance are being implemented to varying degrees in transportation infrastructure systems, but are generally lacking. Infrastructure managers do not currently have the tools to rigorously assess and manage cyber risk. Likewise, limited data and models inhibit the accurate modeling of cyber risk that insurance companies need to offer wider coverage and risk-based rates. Even after improved tools and modeling are developed, residual cyber risk will be significant, and insurance purchase is an important risk management strategy to allow transportation infrastructure systems to recover from cyber events.

We have identified four primary research needs to advance cyber risk assessment, mitigation, management, and insurance for transportation infrastructure systems. The first is the need for cyber incident data and models. The emerging nature of the risk means that historic cyber incident data is limited. The documentation and sharing of cyber incident data is needed to enable better characterization and modeling of the risk. Along with improvements in data documentation and availability, risk models are needed to enable infrastructure managers to understand and target sources of risk and to allow insurers to quantify and rate cyber risks to infrastructure systems.

Secondly, cyber risk metrics are needed to encourage, incentivize, and quantify benefits associated with risk management strategies and mitigation measures. Metrics can assist with the quantification and tracking of risks, and when used as a regular evaluation tool can promote policies, practices, and decisions that enhance the resilience of infrastructure systems to cyber risks. Effective metrics should measure both operational and technical components of the infrastructure system as they pertain to cyber risk, and should also measure outcomes associated with infrastructure system performance during and after a cyber incident.

There is significant literature suggesting that cognitive biases routinely result in the underestimation of risk exposure. The role of cyber risk perceptions and cognitive biases in decision-making about management of cyber risk for transportation infrastructure systems is another research need. Understanding perceived probabilities and impacts of cyber-attacks along with experiences and perceptions of mitigation measures and insurance needs can facilitate the design of strategies to overcome these biases and improve the preparedness of infrastructure organizations for cyber-attacks.

Lastly, research is needed on cyber insurance for transportation infrastructure systems, to support new and more robust cyber insurance products that meet the evolving needs and demands of infrastructure systems. This research should draw from the previously mentioned research needs on metrics and modeling of cyber risk for insurance rating purposes and on cognitive biases and risk perceptions. Research can lead to creative insurance solutions to encourage the purchase of cyber insurance and the adoption of technically effective and cost-effective cyber risk mitigation strategies by transportation infrastructure managers.

Acknowledgments

Support for this research was provided by the Critical Infrastructure Resilience Institute (CIRI). The authors would like to thank the infrastructure managers and insurers who provided valuable insights for this research via their participation in interviews.

References

[1] A. Cox, F. Prager, A. Rose, Transportation security and the role of resilience: A foundation for operational metrics. *Transport policy 18* (2011) 307-317.
[2] B.C. Ezell, R.M. Robinson, P. Foytik, C. Jordan, D. Flanagan, Cyber risk to transportation, industrial control systems, and traffic signal controllers. *Environment Systems and Decisions 33* (2013) 508-516.
[3] G. deSmidt, W.J.W. Botzen, Perceptions of Corporate Cyber Risks and Insurance Decision-Making. The Geneva Papers on Risk and Insurance – Issues and Practice (forthcoming).
[4] C. Toregas, N. Zahn, Insurance for cyber attacks: The issue of setting premiums in context. *George Washington University, 2014*.
[5] T. Bandyopadhyay, V.S. Mookerjee, R.C. Rao, Why IT managers don't go for cyber-insurance products. *Communications of the ACM*, *52* (2009) 68-73.

[6] M.E. Paté-Cornell, M. Kuypers, M. Smith, P. Keller, Cyber Risk Management for Critical Infrastructure: A Risk Analysis Model and Three Case Studies. *Risk Analysis* (2017).
[7] R.M. Clark, S. Hakim (Eds.), *Cyber-Physical Security: Protecting Critical Infrastructure at the State and Local Level* (Vol. 3). Springer, 2016.
[8] M. Nogal, A. O'Connor, Cyber-Transportation Resilience. Context and Methodological Framework. In *Resilience and Risk* (pp. 415-426). Springer, Dordrecht, 2017.
[9] V. Gisladottir, A.A. Ganin, J.M. Keisler, J. Kepner, J., I. Linkov, Resilience of Cyber Systems with Over-and Underregulation. *Risk Analysis 37* (2017) 1644-1651.
[10] Marsh & McLennon, Cyber: The Stakes have Changed for the C-Suite, 2018.
[11] AON, 2018 Cybersecurity Predictions – A Shift to Managing Cyber as an Enterprise Risk, 2018.
[12] AON, Global Insurance Market Opportunities – Insurance Risk Study. 10th edition, 2015.
[13] J.P. Kesan, R.P. Majuca, W.J. Yurcik, The economic case for cyberinsurance, 2004.
[14] K.A. Pesch-Cronin, N.E. Marion, *Critical Infrastructure Protection, Risk Management, and Resilience: A Policy Perspective*. Taylor & Francis Group (2017).
[15] S.M. Rinaldi, J.P. Peerenboom, T.K. Kelly, Identifying, understanding, and analyzing critical infrastructure interdependencies. *IEEE Control Systems*, *21* (2001) 11-25.
[16] E. Frydenlund, A.J. Collins, C.A. Jordan, P.B. Foytik, R.M. Robinson, When the money runs dry: a system dynamics approach to critical infrastructure investment. In *Proceedings of the 49th Annual Simulation Symposium* (p. 8). Society for Computer Simulation International, 2016.
[17] PwC, Aviation Perspectives, 2016 special report series: Cybersecurity and the airline industry, 2016.
[18] B. Chen, C. Schmittner, Z. Ma, W.G. Temple, X. Dong, D.L. Jones, W.H. Sanders, Security analysis of urban railway systems: the need for a cyber-physical perspective. In *International Conference on Computer Safety, Reliability, and Security* (2014) 277-290.
[19] É. Masson, C. Gransart, Cyber Security for Railways–A Huge Challenge–Shift2Rail Perspective. In *International Workshop on Communication Technologies for Vehicles* (pp. 97-104). Springer, Cham., 2017.
[20] S. Romanosky, Examining the costs and causes of cyber incidents. *Journal of Cybersecurity* (2016) 1–15.
[21] J. V. Acker, *Spirit Airlines Pays $7.5M To Settle FACTA Class Action*. October 2015, Retrieved from Law360: https://www.law360.com/articles/719400/spirit-airlines-pays-7-5m-to-settle-facta-class-action.
[22] J.C. Fauntleroy, R.R. Wagner, L.A. Odell, *Cyber Insurance-Managing Cyber Risk* (No. IDA-NS-D-5481). INSTITUTE FOR DEFENSE ANALYSES ALEXANDRIA VA, 2015.
[23] J.P. Kesan, C.M. Hayes, Strengthening Cybersecurity with Cyberinsurance Markets and Better Risk Assessment. *Minn. L. Rev. 102* (2017) 191.