PARTNERS FOR ADVANCED TRANSPORTATION TECHNOLOGY
INSTITUTE OF TRANSPORTATION STUDIES
UNIVERSITY OF CALIFORNIA, BERKELEY

Cybersecurity of Our Transportation Ecosystem

Final Report

February 7, 2022

Partners for Advanced Transportation Technology works with researchers, practitioners, and industry to implement transportation research and innovation, including products and services that improve the efficiency, safety, and security of the transportation system.

This page left blank intentionally

Primary Authors

Brian Peterson
Software Engineering Manager
California PATH
University of California, Berkeley

This page left blank intentionally

TABLE OF CONTENTS

List of Figures

This page left blank intentionally

List of Tables

It is not a matter of if you will be hit by a cyberattack, but rather a matter of how often you will be attacked, how well you have prepared, and how much damage to you and others will result from each attack.

1. Introduction

Cybersecurity has become a critical issue in today's world. In the past, security of our cyberspace was an important issue for some sectors of the economy, especially those dealing with financial information, personal identification related information, corporate systems and trade secrets, government classified information, and other types of data considered valuable targets for hackers. For other sectors, there was much less attention and resources dedicated to protection of our information and control systems. These sectors were often considered less likely to be targeted and a less valuable target.

However, that has changed with time. The growth of cyberattacks such as ransomware attacks where the attacker is likely to encrypt data and withhold access to data or systems while demanding a ransom payment to restore access has made any critical system owned by an entity with significant resources a target. Additionally, critical infrastructure, including water, energy, communication, and transportation or critical services such as healthcare delivery have become targets of choice for criminal attackers with a profit motive, state sponsored attackers, and attackers with a cause (hacktivists). Insider threats pose a fourth source of attacks.

Transportation is not immune to the increase in cyber threats and instead is likely to experience increased attacks. This is likely due to several factors:

- **Limited defenses -** The resources applied to and the pace of improvement in the security of our transportation infrastructure has not kept up with the increasing cyber threats to that infrastructure.
- **Less costly to attack** - The sometimes-poor state of transportation infrastructure systems security often makes an easier target that is less costly to attack.
- **Increasingly critical nature -** Infrastructure systems are becoming more complex, connected, and critical to efficient operation of our transportation system. This trend is very likely to accelerate in the future with increases in digitization, connectivity, and V2X introductions.
- **More profitable attacks** - Infrastructure disruptions may be seen as very profitable. The increase in the critical nature of these systems make them a more profitable target for criminal actors.
- **Increased damage potential** - The increase in the critical nature of our transportation cyber systems increases the potential damage from a state sponsored attack (especially if attacked in tandem with other industry sector attacks such as attacks on our energy infrastructure).

In this report we look at the following elements of securing our transportation system from cyberattacks, including:

- The ways in which our transportation system is vulnerable to cyberattacks
- The level of risk of cyberattacks against our transportation system and risk trends
- Hypothetical and potential attack vectors
- Identification of potential threats
- Possible impacts of cyberattacks against our transportation system

To do this we look at the following:

- Publicly available data on past attacks, both on the transportation sector and other sectors
- Trends within the cybersecurity space

This report intentionally does not include any information on existing cyber defenses specific to any individual organization or entity nor does it include any non-public information regarding past attack events to ensure we did not disclose any information that might increase the likelihood of any future attack. Note also that publicly available attack information is extremely limited due to two critical factors – first, victims of attacks often do not report an attack or are not even aware of the attack and second, victims of attacks do not often disclose details of an attack or the response to the attack.

We also discuss actions that transportation industry actors should take to limit both the likelihood and impact of a successful attack. We discuss issues that impact an organizations' ability to improve their cybersecurity posture.

2. Trends in Cyberattacks and Cybersecurity

Figure 1 displays a recent poll by the Washington Post of its Network experts, "a group of high-level digital security experts from across government, the private sector and security research community" (Washington Post Staff, 2021). The poll reveals that 43% of these experts assert that the United States is more vulnerable, 38% just as vulnerable, and 19% less vulnerable to cyberattacks than it was five years ago.

(Shaffer, 2022)

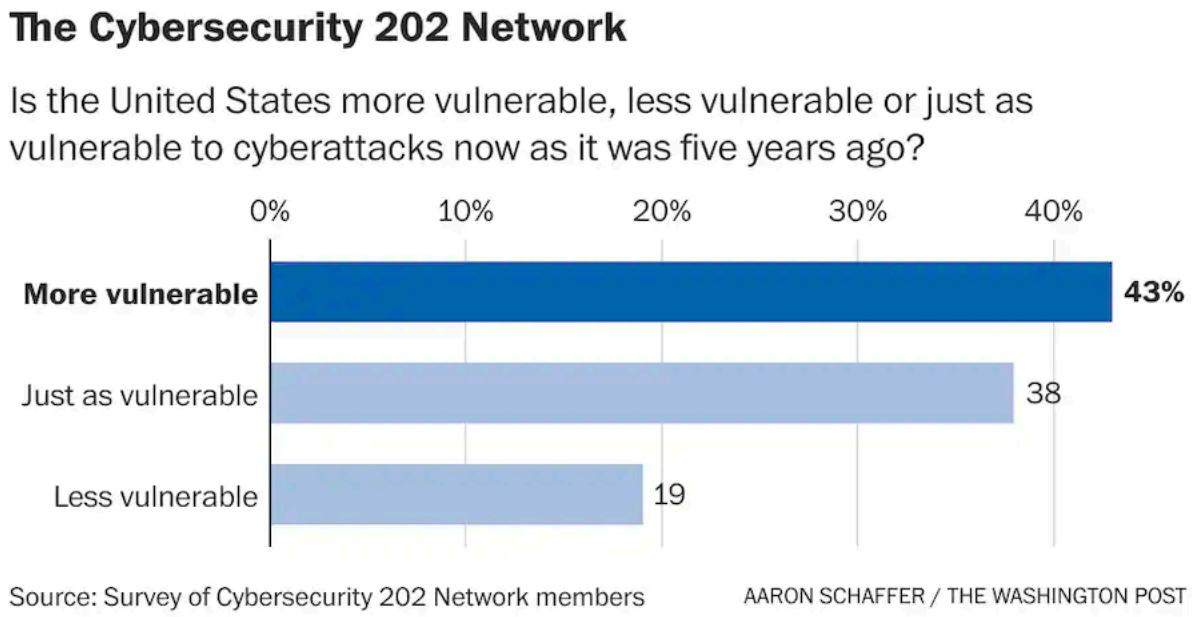

Figure 1 - Experts Weigh in on Relative US Vulnerability to Cyberattack

In general, these experts reveal disturbing trends, including:

- While cybersecurity efforts are generally improving, the threat is growing at a rate faster than our defenses
- The nation has become more dependent upon ever increasingly complex technology and systems
- The systems we deploy and depend upon are often developed with emphasis on function and features and little thought to ensuring their cybersecurity
- There are differences in cybersecurity preparedness and threats between industries and sectors of the economy
- Attacks and attackers are changing, with increases in the monetization and private attackers through ransomware--a significant trend

The transportation sector is not immune to these trends. It is a very attractive, high impact target for attackers that is difficult to defend. The reasons for this include:

- The aging nature of many of its systems
- The complex, heterogeneous, and distributed nature of many field devices with limited security
- Systems are distributed across many different jurisdictions, often with limited cybersecurity expertise
- Significant advances in systems and technologies just being researched and deployed (think automated vehicles and CV2X)
- Significant economic resources at risk (such as freight and pipeline operations)
- Significant safety implications (such as traffic management, maritime operations, or air traffic control)
- The potential national scale disruption that an attack could create

Of particular concern for the transportation sector is that just as the Internet of Things (IoT) is taking off within the sector with Connected and Automated Vehicles, sensing devices, and IP connected infrastructure elements, IoT is also being identified as one of the primary weaknesses of the current cybersecurity landscape.

Quantifying such trends with actual data is particularly difficult. Reporting of cybersecurity incidents is incomplete at best and reporting requirements at a national level have not been required until very recently with the Cyber Incident Reporting for Critical Infrastructure Act (2022) (CIRCIA). Additionally, such reporting is limited to critical infrastructure related attacks and will not be required until the U.S. Department of Homeland Security (DHS) Cybersecurity and Infrastructure Security Agency (CISA) finalizes rules for implementation of the act. At this time, such reporting remains recommended, not required.

2.1. Trends in Frequency of Attacks

In general, the frequency of cyberattacks, as well as losses experienced for an attack are increasing.

Figure 2 provides data from the Center for Strategic and International Studies List of Significant Cyber Incidents (Center for Strategic and International Studies, 2022), illustrating an increase in the number of incidents since 2006. The data collected is limited to those that are publicly reported attacks on government agencies or companies within the defense or high-tech industries, or related to an economic crime of more than $1M. It should not be considered a full list or complete data set.

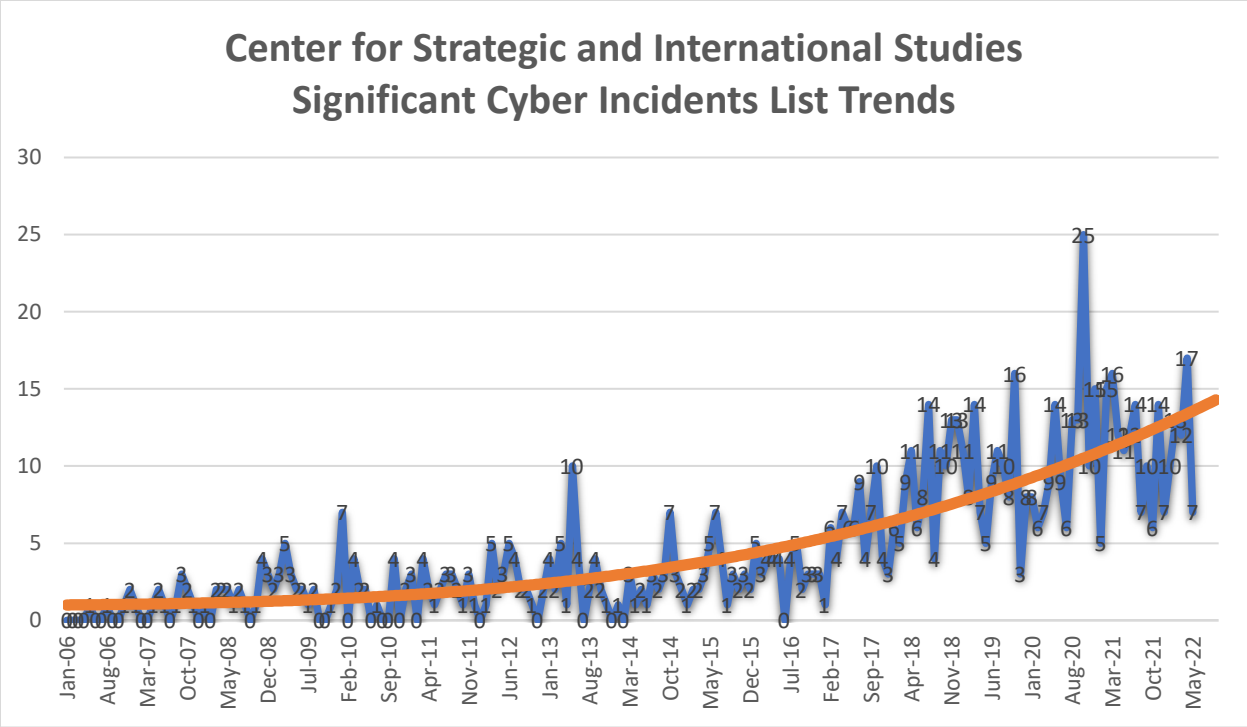

Figure 2 CSIS Significant Cyber Incident Increasing Over Time

Other sources that indicate an increase in attacks include:

- Checkpoint Research indicated a 17% increase in U.S. cyberattacks and a 93% increase in ransomware attacks in the first half of 2021, with a weekly total of 443 attacks within the U.S. The average ransomware payment was reported to have increased by 171%. (Checkpoint Software, 2021) For the full 2021 year, Checkpoint reported a total of 1136 weekly attacks within the government sector, a 47% increase over the previous year, and 501 weekly attacks within the transportation sector, a 34% increase. (Checkpoint Software, 2022).
- The Federal Bureau of Investigation's Internet Crime Complaint Center (IC3) has experienced a steady increase in reported crimes with the number of complaints nearly tripling in the last five years and the losses reported more than quadrupling (Figure 3).

(Federal Bureau of Investigation Interent Crime Complaint Center, 2022)

Figure 3 Increases in Complaints and Losses Reported to US Federal Bureau of Investigation

IC3 reported for the first time in its 2021 report ransomware attacks against critical infrastructure targets (Federal Bureau of Investigation Interent Crime Complaint Center, 2022) with transportation reporting 38 incidences of ransomware attacks and transportation dependent sectors of communications, energy, government facilities, information technology, and financial services reporting a total of 271 attacks (Figure 4).

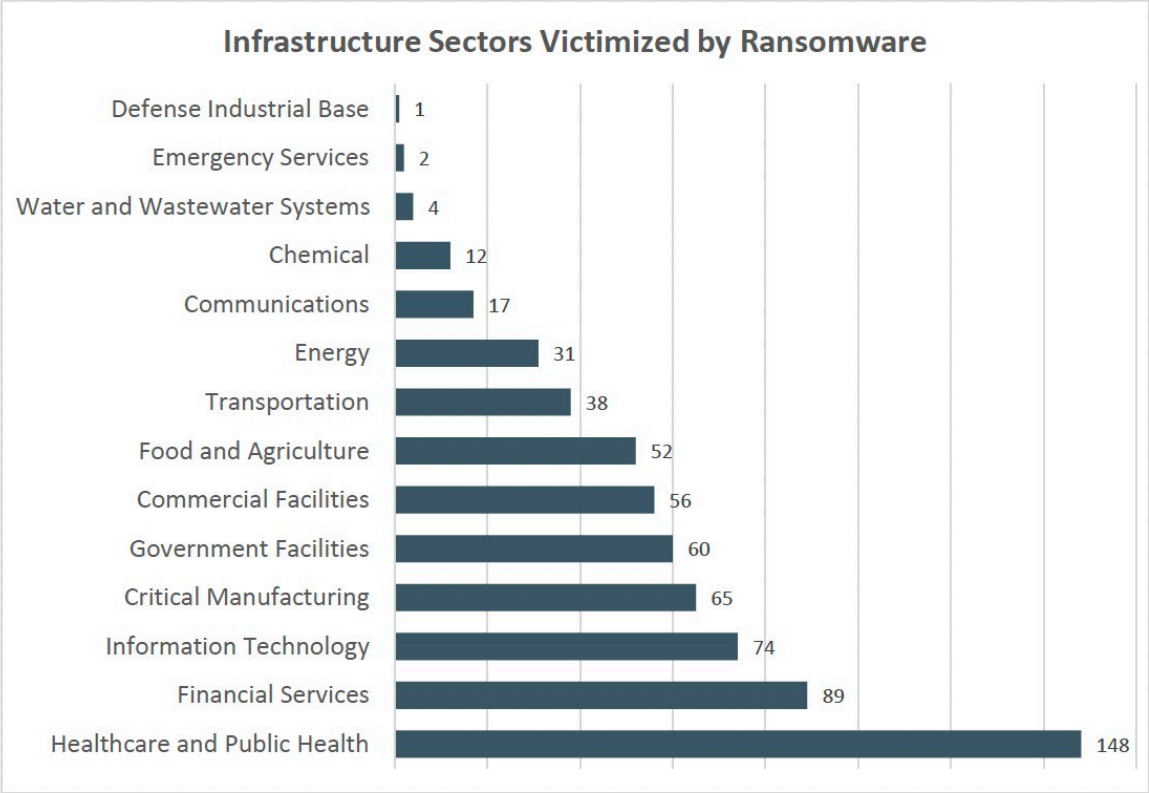

Figure 4 Reported Ransomware Attack by Infrastructure Type - 2021

Total ransomware reports to IC3 reported nationwide increased from 2744 attacks and $29.1M in losses in 2020 (Federal Bureau of Investigation Internet Crime Complaint Center, 2021) to 3729 attacks with $49.2M in losses in 2021 (Federal Bureau of Investigation Interent Crime Complaint Center, 2022). While these include just crimes reported to the IC3 and is by no means a complete set, it represents an increase of 36% in the number of reported ransomware attacks and 69% increase in the losses experienced with a one-year period.

The values reported are highly dependent upon the source, the incidences of cyberattacks are often not reported, and there is no central repository of reported incidences. However, the same trend of increasing attacks and increasing losses is consistent across the industry with no reasonable expectation or reason that the trend will reverse.

Unfortunately, California ranks as having the highest losses of all states within the U.S. and ranks in the top 2 in the number of attacks. (Federal Bureau of Investigation Interent Crime Complaint Center, 2022)

2.2.Trends in Size of Cyberattacks

Size of cyberattacks can be measured in several different ways, including

- Total costs to the victims of the attack, including ransomware payments, costs to identify and remediate impacts of the attack, costs to repair damage from an attack, costs to strengthen protection against attack and improve response to future attacks, operational costs, and costs of 3rd party impacts such as costs for credit monitoring or reimbursement to 3rd parties. Additionally, it may include the costs to inform customers, employees, or others affected by the attack, lost business, costs of lost capabilities and the costs to restore those capabilities, recovery expenses, legal and regulatory expenses, and future direct or indirect costs of an attack.
- Number of systems affected
- Total number of victims affected or records compromised
- Total economic impact across all economic sectors affected

For many of the same reasons that it is difficult to quantify the change in cyberattack frequency including lack of reporting and no single collecting entity, quantifying the change in the size of cyberattacks is difficult at best.

However, there are industry studies that may give some idea of the overall trends in the size of cyberattacks.

2.2.1. Total Cost

IBM provides an annual Data Breach Report (IBM, 2021) (IBM, 2020) to look at the costs of cyberattacks. The report analyzes costs in a number of ways. This report looked at 524 organizations with cyberattack breaches in 17 countries, 17 industries, and interviewed 3200 individuals. Methods to evaluate costs within the report were based on four cost centers; Detection and Escalation, Lost Business, Notification, and Ex-post Response. Cost for a breach varied significantly based on the size of the breach, industry of the victim, type of data affected, and others. The 2020 report indicated that the largest cost driver was the number of records affected which varied from an average cost of $3.86M for breaches of 1M to 10M records to and average cost of $392M for breaches of more than 50M records. The 2021 report indicated the average cost of a breach within the United States was $9.05M. In Figure 5 below (IBM, 2021) provides the cost trend of data breaches world-wide since 2015, with an 11.9% increase since 2015.

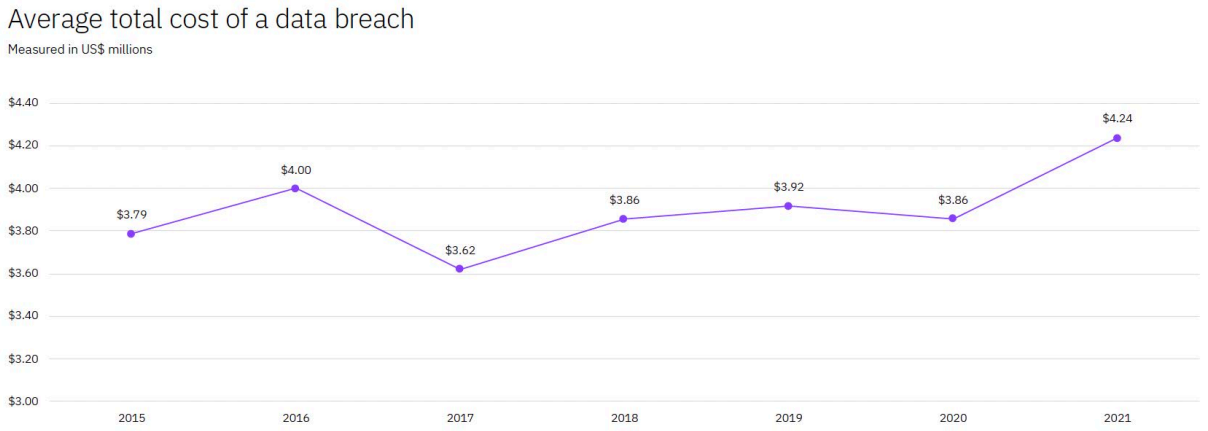

Figure 5 Average Data Breach Cost

Worldwide averages for data breach costs by industry within the IBM report (Figure 6) showed that the transportation sector was at $3.75M/breach, just under the average cost/breach of $4.24M for all industries. As seen below, transportation data breach costs have shown a slight increase since 2020.

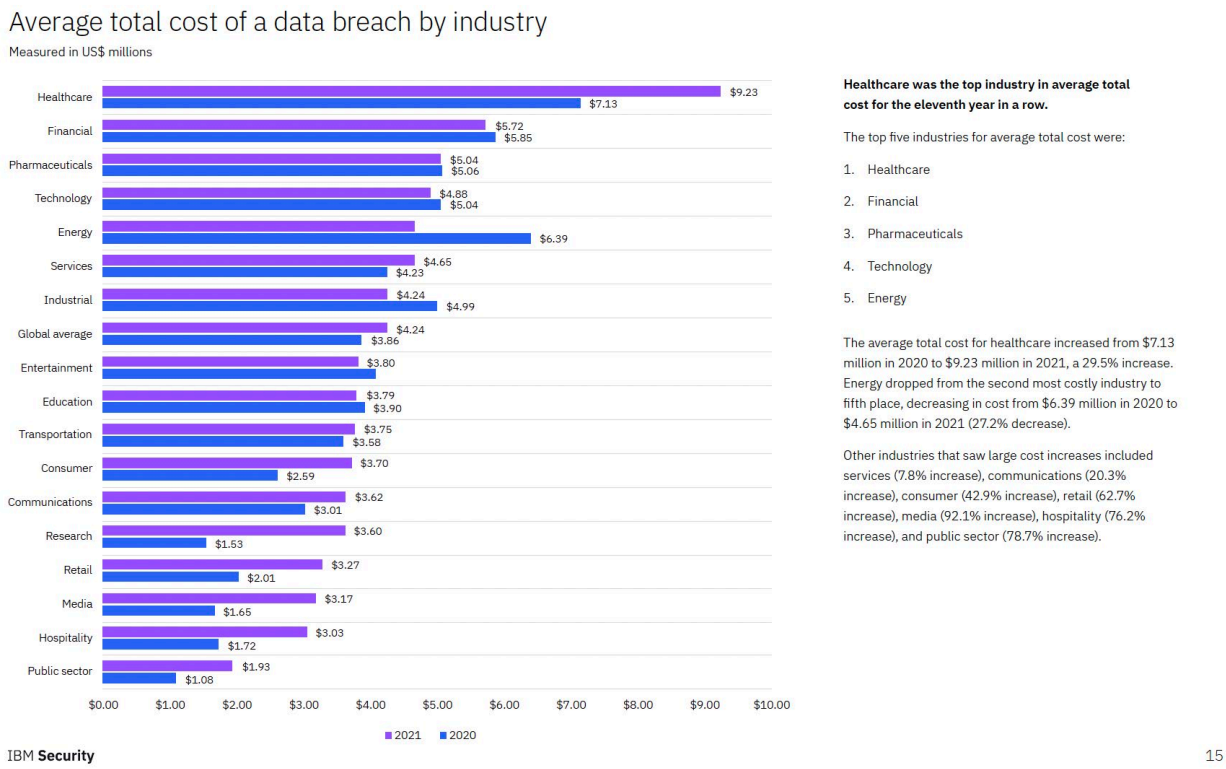

Figure 6 Average Data Breach Cost By Industry

These costs do not include the secondary costs incurred by individuals impacted by the loss of their personal data and are limited to the costs incurred by the direct target of the attack.

2.2.2. Number of Victims or Records Breached

If we look at the trends in the size of attacks based on the number of individuals affected by breaches, namely those customers or individuals whose data was impacted, we see a different trend.

The Identity Theft Resource Center (ITRC) reported in its 2021 in Review Data Breach Annual Report (Identity Theft Resource Center, 2022) that while the number of attacks has had a tendency to increase over time, the number of individual victims of such attacks has seen a decrease over time. Figure 7 provides a view of both compromises and the number of attack victims over the last seven years.

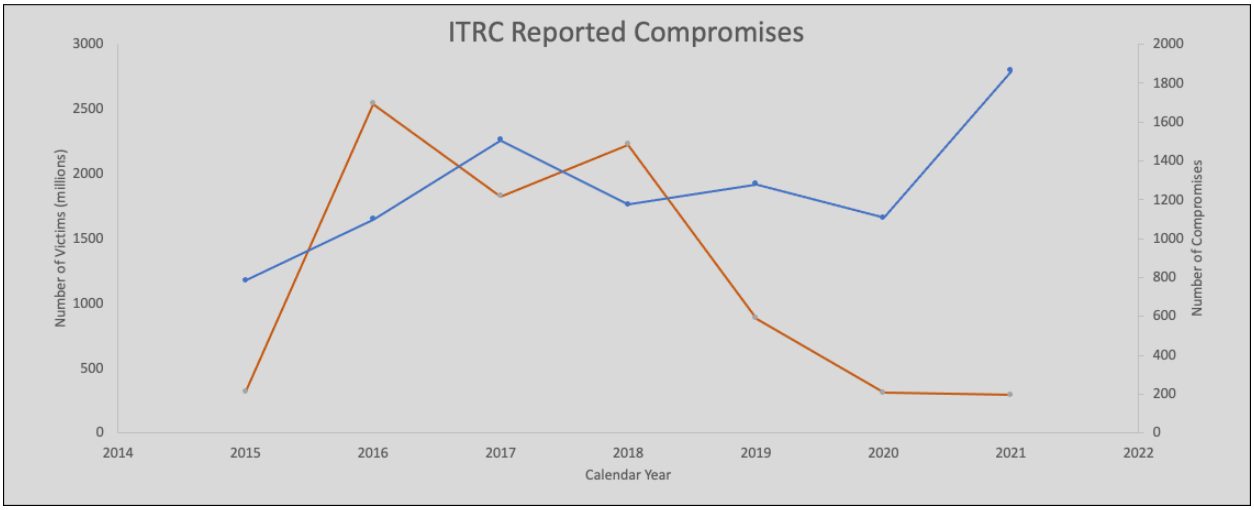

Figure 7 ITRC Reported Compromises and Victim Trends

ITRC also reported that the transportation sector has experienced a similar trend. Figure 8 provides the information for Transportation sector attacks over the last three years.

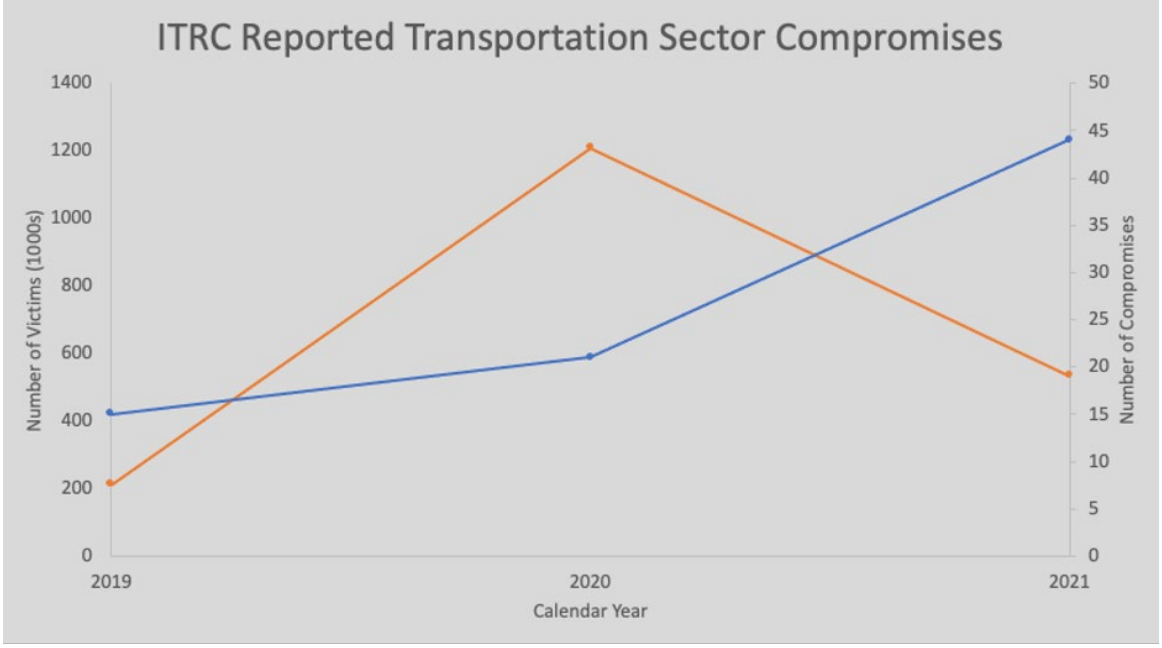

Figure 8 ITRC Reported Transportation Compromises and Victim Trends

Reasons for the increase in the number of attacks while impacting fewer individual records/individuals may include changes in targeting and attack modes by attackers. More directed attacks aimed with specific objectives, such as increases in ransomware attacks targeted at high-value organizations, or attacks that target specific information records or types rather than broad attacks aimed for the largest possible information set may account for this trend.

2.3.Trends in Attack Methods

The types of cyberattacks and attack methods consist of both classic, tried and true methods as well as new and unique attack types and methods. Changes in the target environments, such as the rise of cloud technologies, defense levels and capabilities of targets along with new threat strategies for monetization such as the increase in ransomware, are constantly shifting the methods and targets of attacks.

Table 3-1 provides a classification of cyberattack methods and descriptions.

Table 3-1 Cyberattack Types

Attack Methods	Description
Malware	Involves the use of malicious software on a target device (computer, cell phone, etc.). The attacker must get the user to install the software on the device, often by using tactics such as phishing to get the user to click on a link to initiate the install.

Attack Methods	Description
	Often used as part of the attack strategy for other types of attacks such as ransomware, phishing style, cross site scripting, and others.
Phishing	This attack is executed by sending an email to one or more targets (potentially a mass email) that mimics a source the target will trust. The email contains both a message that solicits an action from the target and a malicious payload such as a link to a malicious website to gather information (such as usernames and passwords) or execute malicious code on the targets computer to gain access to the targets systems. Phishing often involves an element of social engineering to improve the odds of success.
Smishing	A form of phishing attack that uses SMS (text) messaging rather than email to penetrate a target. These often have higher success rates due to more limited defenses established for SMS communications.
Whale phishing	Phishing attacks that target specific high-level targets within specific organizations or pretend to be from such high-level targets.
Spear phishing	Phishing attacks that target a specific individual within an organization.
SQL Injection	A type of attack that utilizes Structured Query Language (SQL) to execute the attack, often in web-based system attacks. The attacker examines the target website for SQL injection weaknesses such as parameters or URL string elements that may be used within a SQL query string in the back end of the web application. The attacker attempts to replace these elements within a custom response to the web application to get the application to execute malicious SQL code. The execution may expose unintended information, damage or delete data on the targeted system, make the web application non-responsive, or cause other damage to the target system.
Ransomware	An attack that obtains access to a target system or systems and encrypts data on those systems such that the systems are unusable. The attacker maintains an encryption key to unencrypt the systems. The attacker may offer to provide the encryption key for a fee, usually cryptocurrency to evade detection, essentially holding the target system(s) and data for ransom. There is often significant damage to the target systems beyond what the encryption key can successfully recover and recovery times can be extensive if the target systems are not sufficiently resilient.

Attack Methods	Description
Double extortion ransomware	A type of ransomware attack where the attacker not only extorts the target not only for the encryption key, but maintains a copy of the data, threatening to expose the data unless the extortion demand is met.
Triple threat ransomware	A type of ransomware that not only extorts the target for both the encryption key to restore access to the attacked systems and to ensure privacy of the data captured, but also demands ransom from individuals (such as partners, shareholders, private individuals, patients, etc.) whose data may be identifiable within the data captured by the attacker.
Trojan Horse	A type of attack that distributes malicious code within what seems like legitimate applications in order to gain access to the targets system(s).
Malware	Any malicious software that is used to attack a target by getting a user to install the software on their system. This may be accomplished in a number of ways identified in this list.
Birthday	An attack that uses hash algorithms usually used to securely exchange messages. The attacker attempts to duplicate the hash used within the message exchange in order to compromise the message exchange, getting the receiver of a message to accept a message not sent by the intended sender but instead sent by the attacker.
Man-in-the-middle and Eavesdropping	Man-in-the-middle and eavesdropping attacks are characterized by the attacker intercepting network communications between two communicating parties. This allows the attacker to access and potentially modify messages sent between the two parties without their knowledge. Eavesdropping attacks are generally attacks that involve the capture of communications in order to gather information such as usernames and passwords, financial information, or other types of information useful to the attacker.
Internal attacks	Internal attacks are any attack made on an organization's systems by a trusted user within the organization. The user usually has trusted, knowledgeable access to secure systems within the organization making them potentially more dangerous than an outside attacker.
Session highjacking	An attacker takes over a trusted connection session between two parties, emulating one party. The remaining party continues to communicate with the attacker not knowing it is no longer the initial trusted party of the session.

Attack Methods	Description
Denial of service (DoS) and Distributed denial of service (DDoS)	An attacker floods a targeted system with a large number of requests, causing the target's performance to decline or to fail. This causes the target to be unavailable for legitimate requests and may make it vulnerable to other types of attacks. Distributed denial of service attacks use large numbers of systems that have already been compromised by the attacker to send the malicious requests.
Password attack	Any type of cyberattack that involves the attacker gaining access to secure credentials (username and password) in order to gain or elevate access to a targeted system. Any number of methods may be used to obtain these credentials including social engineering, brute force, common default passwords, dictionary attacks or others.
Social engineering	The use of different techniques to convince a user to voluntarily provide information to gain access to a system, such as usernames and passwords. This may involve one or more phishing techniques, impersonation of a trusted entity, or even physical means to obtain the targeted information.
Brute force and dictionary attacks	This attack involves repeated attempts to guess information required to access a system. This usually involves automation to guess a user's credentials, gaining access to a target system or systems. Dictionary attacks are similar to brute force attacks but use lists of known or common credentials or accounts to increase the likelihood of success.
URL interpretation	In this type of web-based attack, the attacker observes the syntax of the URL used by a target system and then creates and uses URLs that follow the syntax to attempt to gain access to additional privileged data, system capabilities, and access.
Zero-day attacks	Zero-day attacks are those that take advantage of system and software vulnerabilities either before the software provider knows of the vulnerability or before an effective patch for the defect is available.
Cross-site scripting	Cross-site scripting are web application-based attacks where an attacker injects malicious scripts into a trusted web application. This may be via message forums, reviews, search results, and other types of user-provided information reflected back to other users of an application. The malicious code is now trusted on other users' web pages and is executed, providing the attacker access to cookies or other private information, potentially altering communications between the user and the server, installation of malware, or other cyberattack payloads.

Attack Methods	Description
Web, mobile, and application vulnerabilities	Web sites/applications, mobile applications, and native applications (Windows/MacOS X/Linux/etc.) have software defects that can be compromised by attackers. These defects are often shared within the attacker community, often before they are known and can be corrected by the software provider.
Supply chain	A supply chain attack is a particularly effective attack at large scale. This type of attack is characterized by an attacker identifying a vulnerability of a particular software component that is often used within many organizations to manage other systems or software applications or is used within many other software packages. The attacker uses the vulnerability to compromise the software supply chain, and can result in significant exposure across many organizations and systems. These can be particularly damaging at a very large scale.
Drive-by attack	This attack involves the use of malicious code on an insecure website or application. The goal is to have the malicious code executed by only accessing the site, without any other user intervention required.
Domain Name System (DNS) spoofing	In this type of attack an attacker takes advantage of the Domain Name System, altering the DNS records of a target and redirecting traffic intended for a specific site to a site constructed by the attacker. The attacker may emulate the legitimate site to collect credentials or other information from users believing they are visiting the legitimate site.
Cryptomining/ Cryptojacking	An attacker obtains access to target machine(s) for the purpose of using the system to mine cryptocurrency. The result of such an attack is significant negative impacts on the attacked systems performance.

Attackers will use whatever type of attack is successful at achieving their desired end goal. Given the constant struggle between attackers and defenders and the changing target environments (new system capabilities, new technologies, new data types and targets, updated defenses, new targets, etc.) the most utilized types of attacks are generally driven by those that are most successful with the largest number of targets and the lowest possible effort/cost. This changes frequently over time.

There are a multitude of lists and reports available from both government and private security firms that detail current trends in attack methods and strategies. Some of the more current and dangerous trends involve the increase in ransomware and software supply chain attacks.

2.3.1. Supply chain attacks

The last several years have seen increases in number, scale, and severity of supply chain attacks. While this type of attack has existed for some time, the 2020 SolarWinds attack exposed how dangerous this type of attack has become. In the SolarWinds attack, the attackers targeted the software company SolarWinds and their product Orion which was used by many IT organizations to manage IT environment performance. The attackers penetrated the SolarWinds network and inserted malware into the Orion product software. SolarWinds unknowingly distributed the malware as a software update to its customer base, distributing the malware to over 18,000 organizations worldwide. These customers included government targets such as the United States Homeland Security, State, and Commerce Departments; companies such as Microsoft, Intel, and Cisco, and others in a multitude of industries. Multiple critical infrastructure entities within the oil, gas, power, and manufacturing industry were known to have been affected. In the transportation industry, the list of potential organizations affected included the San Francisco International Airport. The attack was first discovered by the SolarWinds customer Fire-Eye, a company specializing in cybersecurity that discovered the presence of the malware in its systems. The SolarWinds attack was a nation-state actor supply chain attack suspected of originating from Russia. The full scale of the attack remains unknown, as many organizations affected either don't know they were impacted or have not disclosed their infection. (Canales, 2021) (Zetter, 2020).

Prominent attacks that followed SolarWinds include the Kayesa attack, an attack on the Virtual System Administrator (VSA) from Kayesa, a remote management software system used by many managed IT service providers that serve many clients worldwide. In this attack a zero-day vulnerability was exploited to provide the attackers access to VSA and distribute malware and conduct a ransomware attack. The attacker in this case was REvil, a well-known ransomware gang with significant ties to Russia.

Another prominent supply chain incident was the Log4j vulnerability discovered in late 2021. Log4j is an open source java logging package that is included in many java based software distributions, commercial, privately held, and open-source. Its use is so widespread that it is likely that individuals and corporations use multiple software applications across every possible device multiple times per day. Everything from large scale cloud services, enterprise applications, desktop applications, mobile, and web-based applications use Log4j as part of their software distribution. The vulnerability allowed attackers to execute code remotely on unpatched systems using the Log4j software components. Not only were critical systems impacted worldwide (including the shutdown of a portion of the Belgium defense ministry's network), but significant cost and effort was expended worldwide in order to patch the large volume of software systems that use Log4j. The exact cost and impact is unknown, primarily because many attacks go unreported and there may be many systems that still have not been remediated and are vulnerable to future attacks.

2.3.2. Increases in Ransomware Attacks

An increase in ransomware attacks, changes in the ransomware targets, and the scale of potential negative impacts is part of an unfortunate recent trend. Security magazine reported that ransomware attacks increased by 92.7% in 2021. (Security Magazine, 2022)

Within the transportation industry, the most prominent attack is the Colonial Pipeline attack of May, 2021. Pipelines are designated as critical transportation infrastructure and any impacts to fuel pipelines such as the Colonial Pipeline can have significant and potentially disastrous consequences. Colonial's distribution system moves over 100 million gallons of fuel each day, across 5500 miles of pipelines, approximately 45% of the fuel consumed on the U.S. east coast, and stores 28 million barrels of fuel along its distribution system. (Kempner, 2021) Colonial was attacked with a ransomware attack, shutting down its pipeline system from May 7 through May 13, 2021. The impacts were immediate and severe with both shortages and price spikes of fuel across the eastern U.S. The attacker was an organization known as DarkSide and the ransomware was paid, some of which was recovered by the U.S. Federal Bureau of Investigation. The pipeline systems themselves were not attacked, but about 100GB of data were stolen and the billing systems were encrypted. Since the company could not bill customers and had significant concerns regarding the potential for the hackers to access pipeline control operations, the pipeline was shut down.

Another recent example of ransomware's potential impact on critical services at a national level includes two successive attacks on Costa Rica beginning in April of 2022, one by the Russia based Conti ransomware gang and a second by the ransomware-as-a-service operation HIVE. Conti targeted the government of Costa Rica directly, resulting in the declaration of a national emergency. The Conti attack was centered on the data and systems of the country's Finance Ministry including its digital tax service and customs control. More than 800 servers and several terabytes of data were impacted. Transportation related impacts included effects on exports and imports from shipping container shortages as well as the transition of the country's import and export system to a paper-based system. The result was significant delays in the movement of goods and estimated losses of $38M per day. Conti continued its attacks on the government by attacking other government organizations at the local and federal level. The second attack conducted by HIVE targeted the Costa Rican Social Security Fund and the country's health care system. This attack took health care systems offline throughout the country. (Burgess, 2022)

This page left blank intentionally

3. Impacts on Transportation

As mentioned earlier, transportation, including all facets of the transportation system – air, rail, maritime, road infrastructure, pipeline, and freight and personal mobility/vehicles are not immune to cyberthreats and attacks. Impacts of such attacks can be significant, resulting in disruptions to the transportation system and those elements of society that depend on our transportation system. In addition, attacks on services, supplies, and economic sectors upon which transportation depends can have significant impacts on our transportation system and society.

3.1. Examples of Attacks on Transportation Infrastructure and Their Impacts

Recent cyber incidents demonstrate the potential impacts and the extent of the threat (beyond those mentioned earlier in this report):

In 2021 a supply chain ransomware attack on Greek shipping companies was launched through a maritime IT service provider, impacting multiple customers of the provider. Those affected by the attack were unable to communicate with their ships, agents, and suppliers and lost data in the attack. (The Maritime Executive, 2021; The Maritime Executive, 2021)

In July of 2021, Iran's rail system was attacked, disrupting messages regarding train status. The result was significant disruption to the rail system. Message boards for passengers displayed delay or cancellation messages for passenger trains and urged passengers to call for more information. The number provided to passengers happened to be the Supreme Leader Ayatollah Khamenei's office (The Guardian, 2021). The following day the national transport ministry's website was taken down. The attack was perpetrated using malware capable of changing user credentials, terminate running processes, and complete system actions to disrupt recovery and remediation activities. (Greig, 2021)

Iran was attacked with another attack in October of 2021 on its gas stations. The attack prevented customers from using their subsidized fuel cards at the country's gas stations preventing them from obtaining fuel. (The Associated Press, 2021)

In April of 2021, the New York Metropolitan Transportation Authority's systems were penetrated, likely by Chinese government hackers. While no damage was discovered during the investigation of the attack, it still caused extensive loss for the agency for the investigative and related efforts to characterize and respond to the attack. In addition, the attackers did get access to systems capable of significant impact to transit operations. (Rashbaum, 2021)

In 2016, the San Francisco Municipal Transportation Agency experienced a ransomware attack. (Bing, 2016) The attack forced the agency to provide three days of free rides, impacting fare

systems, payroll, and internal email. A significant contributor to the success of the attack was the continued use of the Windows 2000 operating system which was no longer supported by Microsoft.

On August 10, 2020, the Philadelphia transit system SEPTA discovered an attack on their servers, causing it to shut down its systems to limit damage to its operations (Madej, 2020). Service continued, but riders were required to use printed schedules, employee email communication was disrupted, and some databases were impacted. Employee data was compromised including Social Security numbers. Access to its systems was disrupted for months while remediation and recovery actions were taken.

On May 19, 2020, EasyJet, a U.K. based airline reported a hack of customer information, including the emails of over 9 million customers and credit card data for over 2000 customers (U.K. National Cyber Security Centre, 2020). EasyJet had known of the attack since January of that year but did not report the email information breach to customers until April when an increase in phishing attacks against its customers was identified.

In February of 2018, the Colorado Department of Transportation experienced a SamSam ransomware attack. The attackers encrypted files and demanded a ransom. Colorado DOT shut down over 2000 employee systems in response. Critical services were not directly impacted, but employee operations were significantly disrupted (MIGOYA, 2019). A second attack occurred on March 1, 2018. Eradication of the virus was declared on March 9th (U.S. Department of Transportation, 2019). Other DOTs that have experienced attacks include Texas, Idaho, Massachusetts, Nevada, and Utah (Source – Identity Theft Resource Center database).

In 2018 San Francisco Bay Area Rapid Transit discovered that 86% of over 1000 Cisco devices installed in its Silicon Valley Berryessa extension, instead of being new, were used devices that had been decommissioned in hostile nations previously. These devices were found to have hidden backdoors and a persistent ping sending data to a foreign nation hostile to the United States. The compromised devices were found during acceptance testing of an extension contractor's delivery. (Belcher, JD, MPP, Belcher, Greenwald, JD, & Thomas, MBA, 2020)

These are just a few examples of transportation related cyberattacks. As attack data is incomplete at best with many breaches not reported or, in some cases not discovered, with no clear and complete data source for information, it is impossible to tell precisely how many transportation data breaches have occurred. What is clear is that they are common, expensive, and potentially disruptive for the travelling public.

What is also clear are the actual and potential impacts of these attacks. These include:

- Loss of operational capability
- Loss of revenue (current and future)
- Loss of individuals' data (financial, SSN, medical, contact information, other) including data belonging to the travelling public, employees, partners, contractors, etc.

- Loss of public trust and reputation
- Loss of company value (share price or other measure of company value)
- Investigation, remediation and recovery losses
- Permanent or temporary loss of company or government data

While these may be the worst impacts for many businesses, the transportation sector is considered a critical infrastructure component within our society. For such a critical element of our society there is potential for widespread operational disruptions across the entire economy and potential life and safety consequences from an attack. Additional impacts for the transportation sector include:

- Negative impacts on health and safety of the public
- Secondary disruptions in other industries and economic sectors such as manufacturing, retail, energy, logistics and others
- Negative impacts on regional or national economies
- Significant negative impact on the movement of goods and services
- Loss of life
- Large scale public economic loss
- Significant international trade disruption and economic loss

3.2.Potential Transportation Targets

To understand potential impacts, it is helpful to look at what may be likely targets of an attack. We list some of these potential targets in different transportation sectors, along with some possible impacts from an attack on these targets. Note that this report does not identify how such targets might be attacked, as typical vulnerabilities and attack vectors are discussed in Section 5. However, in this list, how the target might be penetrated is not important. In identifying targets and potential impacts, the assumption is that it is not whether any specific target will be successfully attacked or not, it is rather a matter of when the target will be successfully attacked and how well prepared the target's responsible organization is to contain, respond, and recover from an attack.

Additionally, the attack impacts listed may result in differing degrees of severity that are not listed below. Any successful attack may vary in the scale of its impacts. For instance, an attack on a single airline's operations at a single airport for a short duration may impact only a handful of flights which has limited secondary impacts across the national daily flight schedules and population of passengers. However, a successful attack against a major airport's operations causing significant disruptions in its ability to sustain flight operations could have significant impacts across the entire air transportation network.

There are also examples within this list that illustrate potential targets that are not specifically transportation related, but rather on a system or service upon which transportation depends

and that result in secondary impacts that spill over from the initial attack into the disruption of transportation services. In some cases, an attack on one transportation sector or service may also have secondary impacts on other transportation sectors or services. The Colonial Pipeline attack is an example of just such an attack with impacts both on the pipeline services themselves as the primary impact with secondary impacts across the Southeast US road transportation system as fuel shortages quickly appeared once the pipeline was shut down. A future attack on a major port operations center having secondary impacts on rail and road transportation from the resulting cargo backlogs and possible supply chain and economic impacts is another example of an attack with significant secondary impacts.

This report also does not address the likelihood and scale of a successful attack. The likelihood and degree of success in any single attack depends on a number of factors – the defenses of the target, organizational readiness of the target, resiliency of the target systems, the skill of the attacker, inherent and possibly unknown or unaddressed weaknesses of the target, and the attackers intentions and motives (financial, nation-state disruption, hacktivism statement, or other). Any successful attack can have significant primary impacts on its target, both economic and operational. What has been made quite clear in the Colonial Pipeline attack is that transportation and critical infrastructure attacks can result in significant secondary impacts that are more severe than those of the primary target.

Table 4-1, Table 4-2, Table 4-3, and Table 4-4 below are not an exhaustive lists of possible targets and consequences by transportation sector, but rather a set of examples. Not listed, but applicable to any attack is the economic losses involved in detection, containment, remediation, and recovery activities.

Table 4-1 Rail Transportation Attack Targets and Impacts

Rail Target	Impact
Attack on a train signaling control system	Potential safety impacts with possible derailment or collision resulting in substantial property damage, injury, and death Reduced rail line capacity Economic disruption and revenue loss
Attack of passenger information sources such as web sites, dynamic signs at stations, train scheduling systems, with the intent of disrupting or compromising passenger information and service functions of the web site or devices.	Loss or deliberate compromise of information to passengers Inability of passengers to book train tickets and resulting loss of revenue Passenger confusion, missed trains, etc. Loss or compromise of passenger data, including potentially financial or privacy related data Reduced revenue

Rail Target	Impact
Attack of ticketing or financial transaction systems	Compromise of individual privacy and financial data Loss of revenue Train schedule disruption Loss of public trust Significant disruption to ongoing daily operations
Attack of rail, rail yard/terminal, logistics, and freight management systems	Loss of capability to manage freight operations, resulting in disruption to movement of goods Disruptions to terminal operations Reduced capacity, freight delivery disruption and loss Secondary negative impacts to retail, manufacturing, food production, energy, and other economic and industrial sectors dependent upon rail freight Economic loss
Attack on supporting infrastructure such as fuel supply and fueling capabilities, financial services, road infrastructure, or energy/power suppliers	Disrupted rail operations Economic loss Reduced rail capacity Potential safety implications
Attack on enterprise services including human resources, payroll, time and attendance, or other core enterprise systems/services	Disrupted rail operations Compromise/loss of employee and contractor data
Attack on subcontracted service providers systems	Loss of contracted service and resulting service and operational disruptions Revenue loss
Attack on subcontracted service providers systems or attack on IT/Software supply chain	Data compromise Loss of system capabilities Loss of revenue Inability to continue operations Reduced rail system capacity Economic losses Safety/loss of life consequences Loss of public trust Increased regulation Operational constraints Secondary impacts on customers and passengers

Rail Target	Impact
	Freight impacts including potential losses

Table 4-2 Maritime Transportation Attack Targets and Impacts

Maritime Target	Impact
Attack on supporting services such as tug operations, ports, cargo loading/unloading, rail operations, trucking operations	Cargo disruption Port operations disruption Degraded ability to load/unload cargo Negative local traffic disruptions from truck/rail operation degradation Secondary economic impacts at potentially large scale
Attack on key ship systems such as Electronic Chart Display and Information System (ECDIS), navigation system, sensing systems, GPS, radar, Automatic Identification System, or others. **(Tam & Jones, 2018)**	Degraded control or disabling of ship or ship systems Collision Damage to ship or ship systems Disruption to ship traffic in high-traffic or limited movement areas (ports, rivers, canals, etc.) Cargo delivery disruption Piracy (Karahalios, 2020) Safety/loss of life impacts Loss of communications Loss or exposure of data Secondary economic impacts at potentially large scale
Attack on shipping and logistics companies' logistics management systems, enterprise systems (HR, payroll, purchasing, financial management, others).	Compromise of company, suppliers, customer, and employee privacy and financial data Inability to conduct critical operations or degradations in operational capabilities Loss of revenue Disruption in cargo capacity Financial losses from ransomware or theft Significant disruption to ongoing daily operations Loss of critical or daily communications capabilities Loss or exposure of critical or confidential data

Maritime Target	Impact
	Secondary economic impacts at potentially large scale
Attacks on IT services, management, equipment, or software suppliers.	Compromise of company, suppliers, customer, and employee privacy and financial data Inability to conduct critical operations or degradations in operational capabilities Loss of revenue Disruption in cargo capacity Financial losses from ransomware or theft Significant disruption to ongoing daily operations Loss of critical or daily communications capabilities Loss or exposure of critical or confidential data Secondary impacts from attacks on other connected systems with potential for damage in multiple operational sectors Secondary economic impacts at potentially large scale
Attacks on supplies or services that maritime operations depend upon, such as fuel delivery and operations, road or rail infrastructure and operations, energy and power providers	Disruption in cargo operations and degraded capabilities Backlog in cargo operations Secondary truck or rail cargo operations impacts Safety impacts Secondary economic impacts at potentially large scale
Attacks on government agencies and services such as customs, emergency first responders, and other local, state, or federal government service and support agencies	Interruption or disruption of international cargo operations Secondary economic impacts at potentially large scale Reduced cargo capacity and operations Negative impacts to safety and emergency response Physical security impacts Disruptions in inspection and customs operations
Attacks on ship building and maintenance operations	Degraded control or disabling of ship or ship systems

Maritime Target	Impact
	Collision Damage to ship or ship systems Disruption to ship traffic in high-traffic or limited movement areas (ports, rivers, canals, etc.) Cargo delivery disruption Piracy Safety/loss of life impacts Loss of communications Loss or exposure of data Secondary economic impacts at potentially large scale

Table 4-3 Air Transportation Attack Targets and Impacts

Air Target	Impact
Attacks on aircraft systems such as flight management systems, controls, propulsion, navigation, communications, safety systems, and others (Note that there are no confirmed successful attack on an aircraft, but attempts have been made in the past **(Freiherr, 2021)**	Potential life and safety impacts on passengers and crew Loss of use of aircraft assets Financial loss Reputational loss Identification, remediation, and recovery costs Engineering and modification costs for fleet remediation
Attacks on air traffic control	Air traffic control disruptions Reduced air traffic capacity Ground traffic control disruptions Reduced ground traffic operations and capacity Decreased takeoff and landing capacity Potential life and safety impacts, collisions Damage to aircraft Disruptions to air traffic communications Degraded situational awareness by ATC and aircrews
Attacks on airline operators	Customer, operator, supplier data loss Privacy and financial data loss Disrupted operations Revenue loss

Air Target	Impact
	Ticketing and boarding disruption Financial loss Negative reputation impacts Disrupted baggage operations Disrupted flight operations Flight crew impacts Employee data loss Enterprise operational impacts including HR, payroll, financial systems, business operations systems, and other system disruptions Airport operations disruptions Secondary impacts on other airlines' operations and customers, systemwide flight disruptions Secondary impacts on suppliers, contractors, partners, servicers operations and capabilities Air cargo and delivery service disruptions
Attacks on air cargo operators	Customer, operator, supplier data loss Privacy and financial data loss Disrupted operations Revenue loss Financial loss Negative reputation impacts Disrupted flight operations Flight crew impacts Employee data loss Enterprise operational impacts including HR, payroll, financial systems, business operations systems, and other system disruptions Airport operations disruptions Secondary impacts on ground cargo operations and customers Secondary impacts on suppliers, contractors, partners, servicers operations and capabilities Air cargo and delivery service disruptions
Attacks on service providers such as fuel services, catering services, aircraft ground	Disruptions to cargo and passenger air service

Air Target	Impact
operations services, baggage handling, other support services	Delays or disruption to baggage handling and other passenger services Systemwide flight disruptions
Attacks on IT service, software, and equipment providers	Disruptions to cargo and passenger air service Delays or disruption to ticketing, boarding, baggage and other passenger services Systemwide flight disruptions Air safety implications Loss of revenue Damage to public perception Loss of data Loss of privacy and financial information
Attacks on aircraft and parts suppliers, maintenance services	Delays in aircraft delivery, maintenance service schedules Corrupted flight maintenance records (note most recordkeeping in aircraft maintenance logs remain on paper, limiting but not eliminating such risk) Air safety implications
Attacks on ticketing services, including travel agency service providers and booking agencies	Customer, operator, agency data loss Privacy and financial data loss Disrupted operations Revenue loss Ticketing and boarding disruption Financial loss Negative reputation impacts Employee data loss Enterprise operational impacts including HR, payroll, financial systems, business operations systems, and other system disruptions Secondary impacts on suppliers, contractors, partners operations and capabilities
Attacks on government agencies and services such as customs, TSA and other security services, emergency first responders, and other local, state, or federal government service and support agencies	Flight disruptions Security impacts International air cargo disruptions Passenger delays Privacy data loss

Air Target	Impact
Attack on supporting infrastructure services such as road infrastructure, energy and power, freight and trucking, or others	Secondary impacts on passenger and cargo operations

Table 4-4 Road Transportation Attack Targets and Impacts

Road Target	Impact
Attacks on traffic control infrastructure such as traffic management systems, intersection signals, ramp meters, traffic sensing	Increased traffic disruption and delay
Attacks on traffic management centers	Inability to respond to traffic and vehicle events Increased traffic disruption and delay Potential negative impacts on individual and public safety Potential negative impacts on critical public emergency response such as evacuations
Attacks on individual vehicles, vehicle fleets, or large numbers of vehicles via over-the-air updates, vehicle connectivity compromise, or supply chain attacks.	Negative life and safety impacts Disruption of vehicle operation, potentially during vehicle operation Disruption in vehicle fleet operation, with potential secondary impacts depending upon type of vehicle (freight, local delivery, passenger, etc.) Loss of vehicle use for unknown time period
Attack on supporting services such as electrical grid, fuel, freight and trucking, financial services, or others.	Loss of use of transportation system Loss of revenue (toll revenue, fuel tax revenue) Financial loss Loss of critical transportation services Economic disruption Damage to public perception Loss of data Loss of privacy and financial information
Attacks on CV2X infrastructure elements (future)	Loss of data Loss of privacy information Inability to respond to traffic and vehicle events Increased traffic disruption and delay

Road Target	Impact
	Potential negative impacts on individual and public safety
Attacks on tolling operations	Loss of revenue Damage to public perception Loss of data Loss of privacy and financial information
Attacks on IT service, software, and equipment providers	Loss of revenue Damage to public perception Loss of data Loss of privacy and financial information Inability to respond to traffic and vehicle events Increased traffic disruption and delay Potential negative impacts on individual and public safety

3.3.Secondary Impacts

While the impacts of any attack on a specific target can be significant, both economically and operationally, it is the secondary impacts that can be most severe and are often overlooked in risk assessments. In general, the subject of the primary attack will concentrate on minimizing both its own economic, operational, and reputational losses. However, the ability of the subject of the primary attack to address secondary impacts are likely limited at best and may not be in its best financial or other interests beyond what is legally required.

The transportation sector may be either the cause of secondary impacts, the victim of secondary impacts, or both. Any successful strategy to address cybersecurity and the impacts of an attack must address each of these potential scenarios.

4. Vulnerabilities and Attack Vectors

To understand how to address cybersecurity within our transportation system, we must understand where the system is vulnerable and what attack vectors exist to exploit those vulnerabilities. There are some vulnerabilities that are more prevalent within the transportation sector than other critical infrastructure or economic sectors, but all are common given the nature of cybersecurity and how cyberattacks are carried out.

Cyber defense, consulting, tools and software, education, and services are, of course, a significant IT services and products industry. What might be surprising is that cyberattacks are their own industry today, with cyberattack as a service, cyberattack tools and software, hostile government cyber forces, and even complex business enterprises (with HR, recruiting, complex financial and money laundering operations, employees, payroll, etc.) (Check Point Research, 2022) that conduct cybercrime all part of the offensive cyber landscape. These offensive actors utilize many different attack methods, often in combination, to attack vulnerable systems and operations and target those entities that specifically align with their attack objectives. They are often very complex operations that develop complex and effective tools and strategies to take advantage of well-known weaknesses in the systems they target. They are constantly identifying new weaknesses, strategies, and methods, making defense against these attacks extremely difficult, expensive, and complex. The complexity and reactive nature against new attack strategies make it impossible to defend against every attack.

There are many common technical vulnerabilities within the systems that make up our transportation system such as misconfigured networks or software, software that has not been updated with the latest security patches, zero-day bugs within installed software, or others. However, these often exist only because of the vulnerabilities present within our organizations that are responsible for these systems that are under attack.

4.1. Vulnerabilities Identified in Investigations of Past Attacks

To understand and appreciate the importance of addressing even the simplest of vulnerabilities, one must look at how past attacks have been perpetrated. Attacks may involve the exploitation of a single vulnerability or multiple vulnerabilities. As previously stated, many attacks are not reported, and in many cases that are reported, the specific mechanism of attack is not disclosed. However, the following case studies offer an understanding of how these specific attacks were carried out and illustrate how addressing vulnerabilities is critical to defense against such attacks. Both case studies have well known and recommended actions that would have prevented or limited the damage from the attack, had they been used.

4.1.1. Colonial Pipeline (2021)

The Colonial Pipeline is one of the single most impactful cyberattack on the transportation sector that has occurred to date. Impacts included not only operational and financial impacts

on the target company itself, but extensive secondary impacts on fuel supplies and the transportation network that depends upon them across a significant geographic area of the United States. The attack was a ransomware attack perpetrated by the hacker organization DarkSide, which operates out of Eastern Europe or Russia. Investigation indicated and the company reported that the attack was the result of stolen credentials from a previous data breach that had been "reused" (when an individual utilizes the same credentials for multiple accounts/purposes) and that the VPN that was breached with those credentials may have been a legacy VPN that was no longer actively used. (SecureLink, 2021) Two-factor authentication was not in use.

Actions that would have prevented this attack include:

- Educating users to use unique credentials for each account, to use services that inform users when credentials are found in circulation on criminal networks, and to change credentials when credentials have been exposed.

- Use two-factor authentication.

- Remove software and services from computers and networks when they have reached their end-of-life or are not required. Software and services that expose attack surfaces should only be installed and available when required and only to authorized users with a need for their use.

4.1.2. NotPetya (2017)

NotPetya is malware that originated as part of a state-sponsored (Russia) attack perpetrated initially on the Ukrainian government and businesses that spread worldwide. The attack resulted in significant impacts, both operationally and financially, on many economic sectors including transportation. NotPetya's origins included a leaked National Security Agency tool, EternalBlue, that took advantage of a flaw in Microsoft Windows (patched by Microsoft prior to the attack) attacking the system boot sector and file management systems and malware called Mimikatz that, once installed, was able to retrieve passwords from a computer's RAM. With those credentials MimiKatz could compromise other machines on the network. NotPetya then effectively destroyed the infected system and continued to do the same across any network connected computer. (Greenberg, 2018) (Capano, 2021)

What NotPetya depended upon was systems that had not been updated with the patch released by Microsoft. In fact, it only needed one such system, as once one was infected, it obtained credentials to infect others even if they were patched. These capabilities to penetrate an entire network of systems and the fact it was built by a state actor with the intent to destroy every infected system made it particularly damaging worldwide.

Transportation impacts included the near complete destruction of the shipping company Maersk's computer systems and the shutdown of their operations across the world. Maersk held 19% of shipping capacity market share in 2017 (A.P. Moller - Maersk, 2018). Maersk shutdowns at ports resulted in significant backlogs of truck traffic at the affected ports. The attack led to the inability to use Maersk's systems to schedule shipments, affected their phone networks, and resulted in the need to completely rebuild Maersk's IT infrastructure. Maersk's infection was traced to a single install of an accounting package provided by a Ukrainian software and IT service company. NotPetya also affected shipping in Europe, infecting TNT Express, costing FedEx $400M. Maersk indicated its costs were $300M. Non-transportation victims of the attack included hospitals, Merck (pharmaceuticals) ($870M in losses), and the Chernobyl nuclear power plant.

Actions that would have prevented or limited the impact of NotPetya include:

- Regularly and timely updates to software and systems across an organizations network
- Network segmentation to limit the reach of such attacks.
- Supply chain defenses and better security practices within IT software and service providers
- Eliminate access of non-patched or unmanaged computers to critical IT infrastructure

4.2.Common Vulnerabilities

Most attacks are directed at and often successful against common, well-known vulnerabilities that are not sufficiently addressed within organizations and systems. Attackers scan for these weaknesses, use them to design, develop, and test their strategies, tools, and methods, and count on them to successfully execute their attacks.

Vulnerabilities may include:

- Individual and specific operating system or software vulnerabilities
- Specific common attack surfaces
- Organizational or individual attack surfaces
- Specific attack vectors

This paper defines a vulnerability as weaknesses in an organization's cyber defenses and in response and recovery capabilities. These can be classified into technical, personal, and organizational vulnerabilities. Technical vulnerabilities include those that are inherent in an organization's IT infrastructure; its servers, networks, workstations, software, operating systems, hardware/network/software cyber defenses, etc. Personal vulnerabilities are those inherent in people resources – the individuals that have access to an organization's information

technology assets. These include not only those who belong to the organization itself, but customers, partners, contractors, and any other individuals who interface with the organization's IT assets. Organizational vulnerabilities are those that are inherent within the organization itself – its culture, priorities, budgets, training programs, leadership, controls, policies, staffing, and others. Some vulnerabilities will cross these boundaries. For example, access control management (the practice of ensuring only those individuals who need access to a specific IT asset or capability are granted such access and those without such a need are restricted from such access) may have elements in all three:

- Automated removal of accounts for personnel that have changed responsibilities or have left an organization (technical)
- Ability to sufficiently delineate and isolate permissions to an IT asset or service (technical)
- Automatic removal of non-required services on desktop/laptop builds (technical)
- Continuous monitoring of IT assets or services with automated notification of unusual or unauthorized access and automated response actions to such access (technical)
- Organizational policies that define processes required to grant and revoke access to restricted assets (organizational)
- Ensuring sufficient staffing and budgets to execute actions required to ensure sufficient access control management (organizational)
- Proper implementation of access controls and following of good practice when accessing restricted IT assets or services (such as using separate admin and personal accounts when using IT assets and services, using admin accounts only when admin access is required)(personal)
- Using unique credentials and not using common credentials across accounts (personal)
- Not sharing credentials with other individuals (personal)
- Training all users in organizational access control policies and proper use of IT assets and services (organizational)

Common technical vulnerabilities include:

- Insufficient network segmentation, protection (firewalls), and poor network design or implementation
- Network and firewall misconfiguration
- Out of date OS and software updates, high OS/software patch latency (defined as the time between the release of an update and the completion of its installation across the entire organization)
- Poor software or hardware supply chain controls
- Use of remote desktop protocols/software
- Poor software lifecycle controls, hidden use or installations of legacy or unused software and software components
- Poor access control management
- Poor network and system monitoring and alerting capabilities or practice

- Lack of resiliency in system architectures and implementation
- Lack of redundancy within critical systems or systems they depend upon
- Poor backup practices
- Lack of immutable backups
- Poor security configurations
- Software misconfiguration
- Cloud services misconfiguration
- Software vulnerabilities and insecure software development practices
- Improper use or lack of understanding of shared responsibility models
- Insufficient use of encryption (data in motion, data at rest)
- Lack of use of two-factor authentication
- Inappropriate trust relationships and configuration
- Use of legacy systems and software that are beyond their end-of-life

Common personal vulnerabilities include

- Using common credentials across multiple accounts
- Continuing to use known compromised credentials
- Lack of appropriate and sufficient knowledge regarding cybersecurity relative to an individual's role, tasks, and responsibilities within the organization
- Poor individual cyber hygiene (clicking without thinking, etc.)
- Sharing of credentials between users

Common Organizational Vulnerabilities

- Lack of senior leadership understanding of security risk, potential impacts, threats, and costs
- Insufficient prioritization of IT security
- Lack of understanding or usage of organizational risk management
- Insufficient personnel training to spot attacks such as phishing attempts
- Insufficient IT security staffing resources (budgetary, availability, or other)
- Lack of specialized IT security training and specialists within IT organization
- Insufficient IT security funding or lack of dedicated security resources
- Inadequate or lack of IT security leadership and allocation of responsibility and authority
- Insufficient security auditing and review
- Insufficient physical security
- Inadequate resources to maintain or replace legacy systems beyond end-of-life
- Insufficient organizational cybersecurity capability or capacity or lack of understanding of existing capacity and maturity
- Inadequate risk management practices

4.3.Special Vulnerabilities Common in Transportation

Much of the transportation sector has several characteristics that make it particularly vulnerable to cyberattack. These include the following:

- A significant population of legacy equipment and devices resulting from both long equipment life cycles and lack of attention and funding to update and replace aging systems and devices
- A recent entry into the digitization space, with limited experience and understanding of the need to secure digital assets and how to mitigate the resulting risks resulting from increased data collection, automation, and digitization
- Lack of budgets, staffing, and expertise to address cybersecurity issues, especially within government and smaller companies
- Significant increase in technology innovation and the connectivity of the transportation system with increasing demands on mobility, energy efficiency, data volume and capabilities, and technology development and improvement

Transportation organizations are under increasing pressure to focus on technology solutions, connectivity, new sources of data, new mobility solutions, improved systems and capabilities, and new services for users and consumers of transportation services. Often these pressures tempt organizations to focus on service delivery and functionality of new systems and software with reduced focus on the security of these new services and systems. New technology, systems, and capabilities often take priority over ensuring existing transportation assets are maintained and secured and that organizations are prepared for and respond appropriately to cyberattacks.

Legacy equipment with long life cycles is a critical vulnerability within the transportation space. In some cases, outdated systems remain installed within critical infrastructure. This is often a result of connected physical equipment that cannot operate with updated operating systems, firmware or software that remains in operation without support contracts, and in some cases the providing vendor no longer supports the software or is no longer in business. Examples include multiple naval and maritime ship systems continuing to run Windows XP to maintain compatibility with ship hardware (some nations' military hardware using older Microsoft operating systems pay Microsoft to continue support for the product) and Maersk identifying Windows 2000 Servers continuing to operate up until the NotPetya attack despite no longer receiving security updates from Microsoft (Greenberg, 2018). This is an extreme example that goes well beyond the simple case of missing a few software patches over a period of months.

Connectivity between transportation systems and field devices, as well as between multiple agencies and central systems, is still limited within the transportation space. In some ways, this is an advantage – systems that are not connected are very difficult to attack and often require a physical presence. However, organizations that are connecting systems and field devices are

often not fully aware of the cybersecurity implications of such connectivity and are often missing the expertise required to secure those systems. Often the functions, requirements, and benefits of such connectivity and the stated project goals take precedence over cybersecurity in projects that connect infrastructure elements, leaving cybersecurity as a second-tier concern or worse. Program budgets may not include specific allocations for cybersecurity issues.

This page left blank intentionally

5. Dependencies

The most damaging cyberattacks are often more damaging in their secondary impacts than they are to their primary target. Examples of this include the Colonial Pipeline and NotPetya attacks, their primary targets being the Colonial Pipeline company and the Ukrainian government, respectively. The secondary damage that resulted from these attacks; the shortage of fuel and impacts on transportation in the Southeastern U.S. in the Colonial Pipeline attack; and the massive impacts across multiple worldwide businesses and the costs to recover, including significant impacts to transportation and freight in the case of NotPetya, were significantly greater that the impacts to the primary targets.

The reason for this is the interdependent nature of our world economy. Transportation plays a key role in these dependencies, not only because it is "critical infrastructure", but also because so much of the world's economy depends upon transportation. Transportation, in turn, has significant dependencies within itself and on other sectors of the world economy.

To illustrate these dependencies, and to perhaps see where significant secondary impacts are likely to occur, a diagram may be beneficial. The diagram will not attempt to identify every possible dependency, but rather attempts to illustrate how an attack on one element of one sector of transportation or perhaps a service that supports many sectors may ripple into other sectors of the transportation system and the economy. The diagram also is based on very broad elements of the transportation system that may represent many different organizations, systems, users, and their own internal dependencies.

Let's start with five primary, high-level transportation sectors (Pipelines, Air Transportation, Road/Ground Transportation, Rail, and Maritime Operations) (Figure 9).

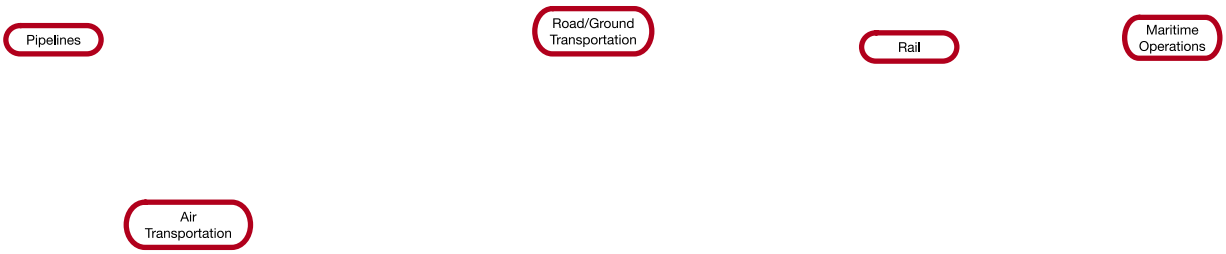

Figure 9 Dependency Diagram (Primary Transportation Sectors)

Next, let's add a primary function of our transportation system, the ability to move goods (freight) and look at the dependencies to each of the different sectors (Figure 10).

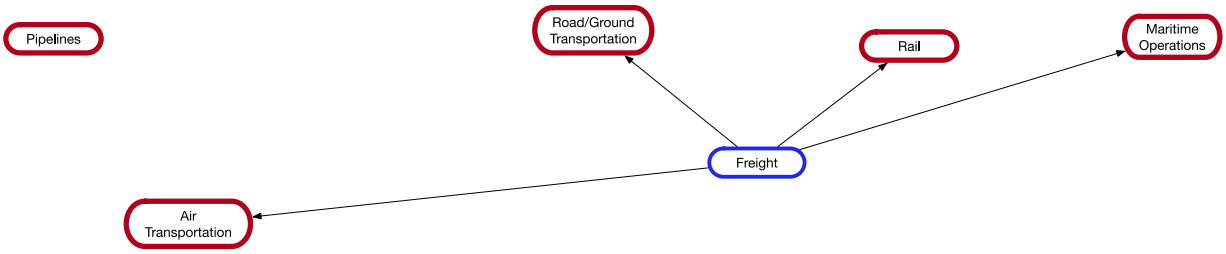

Figure 10 Dependency Diagram (Adding Freight)

What is simply evident is that the ability to move freight within our economy is dependent primarily on our Air, Road, Rail, and Maritime transportation system. Certainly, these dependencies are not a surprising finding. The diagram does not attempt to capture every possible dependency, as it would be unreadable. For example, pipelines are also usually classified as transporting freight, generally liquids and gaseous materials. Also note that the arrows point in the direction of dependency (Freight is dependent upon each of the different modes of transportation. Often the dependency is actually in both directions in the diagram, but for simplicity, this is not always illustrated. What we can assume is that through these lines between sectors and services, the secondary impacts of a cyberattack travel. An attack on freight services can impact one or more of the connected transportation sectors.

Now add some additional transportation elements (Figure 11). Again, these are broad categories and not representative of all possible elements.

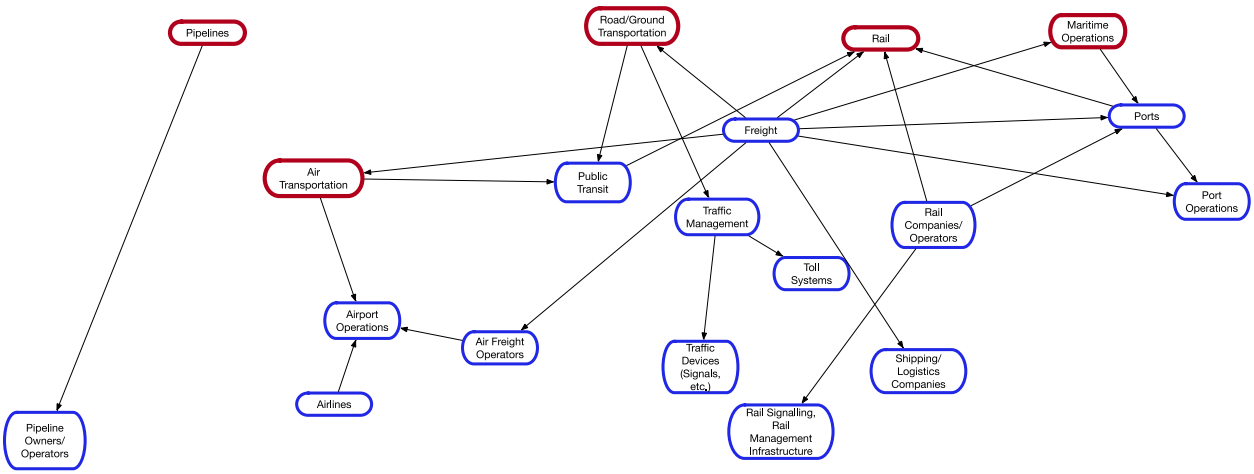

Figure 11 Dependency Diagram (Transportation Elements)

Here some internal transportation element dependencies become visible. Maritime operations depend upon ports which depend upon port operations (port operators, port authority, contactors, etc.). Rail companies and operators depend upon a rail transportation system and the signaling and other infrastructure that make it possible to run a rail system. Road and ground transportation depend upon traffic management (DOTs, TMCs, contractors, service providers, consultants, maintenance crews, etc.) which depends on different infrastructure devices such as intersection signals, signs, and sensors as well as tolling systems for funding and more recently as a demand management strategy. Road and ground transportation depends

also on public transit, upon which air transportation may also depend upon to transport passengers to the airport. Air transportation also depends upon airport operations and airlines. Freight depends upon air freight operations which depends on airport operations. Our system of pipelines depend upon pipeline owners and operators. Freight, which has links to the primary transportation sectors directly and in turn is linked to nearly every element in the diagram, is dependent upon shipping and logistics companies. What becomes evident is that the connections between these different elements are highlighting potential paths of secondary impacts of a cyberattack and the ways in which an attack on any element of the system can spread across the system in what may otherwise not be apparent. An attack on maritime port operations can impact the ports themselves which can impact rail and ground transportation systems. The reality is that many of these dependencies actually flow in both directions and rail or ground transportation disruptions could impact maritime operations as well.

All of the organizations, people, systems, and services represented within these transportation related categories are also dependent upon government services (Figure 12). For a few transportation related examples, the diagram includes law enforcement, emergency services, customs, Transportation Security Agency (TSA), and air traffic control.

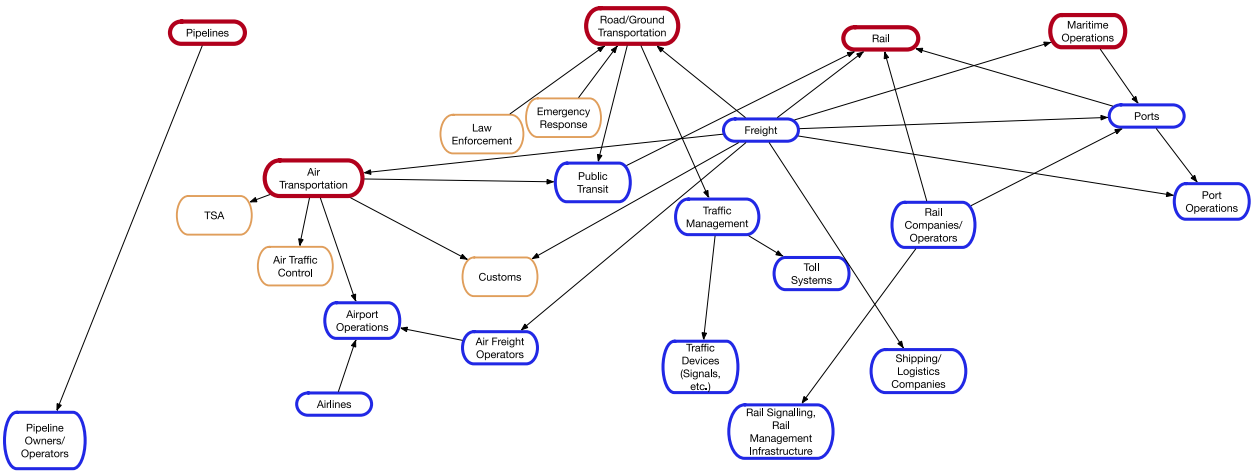

Figure 12 Dependency Diagram (Government Services)

Key to these government services and the dependency the transportation system has on these is the ability of an attacker to disrupt the transportation system by disrupting government services. One can consider as an example the disruption in the state's ability to maintain the movement of freight during an attack on the systems of the U.S. Customs and Border Protection or those of customs brokers. Government services are key targets of nation-state cyber attackers, and economic disruption as well as critical infrastructure disruptions are key objectives of such attackers.

Next are other services outside of the transportation sector upon which transportation depends (Figure 13).

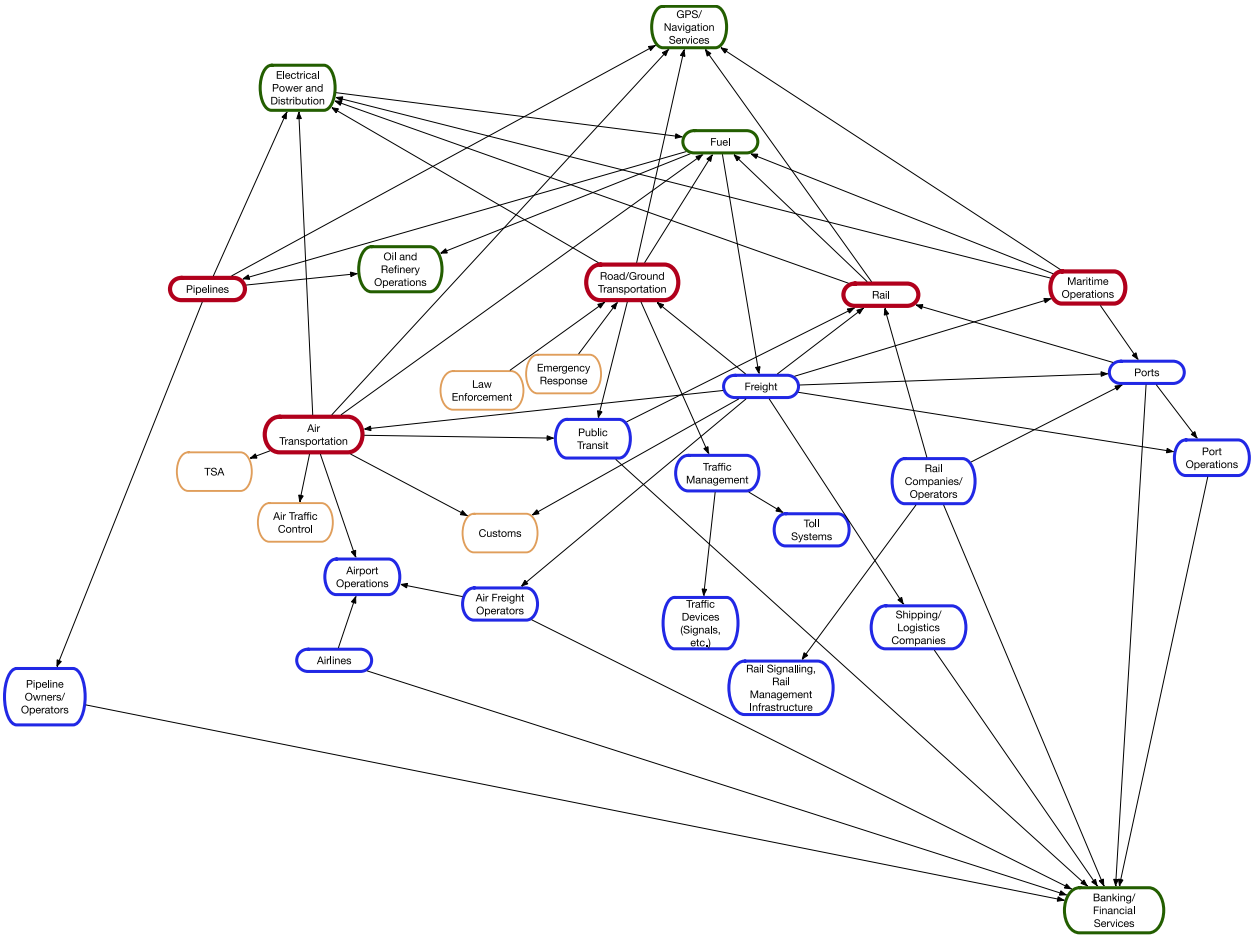

Figure 13 Dependency Diagram (Other Services)

Here added to the diagram are representative services such as banking and financial services, electrical power and distribution, fuel, oil and refinery operations, GPS and navigation services. Each of these large categories of services and industries themselves could have their own dependency diagrams. What becomes evident in adding these is that attacks on industries and services can impact multiple elements of the transportation system. Again, the dependencies can work in both directions; an attack on freight systems can impact fuel deliveries and an attack on fuel supplies can impact freight operations. What is also clear is that there are some services that have connections to many different points in the diagram (fuel, banking, power), making an attack on these services potentially more impactful.

Lastly, the diagram adds our IT services that are critical to our transportation system and other sectors of our economy (Figure 14).

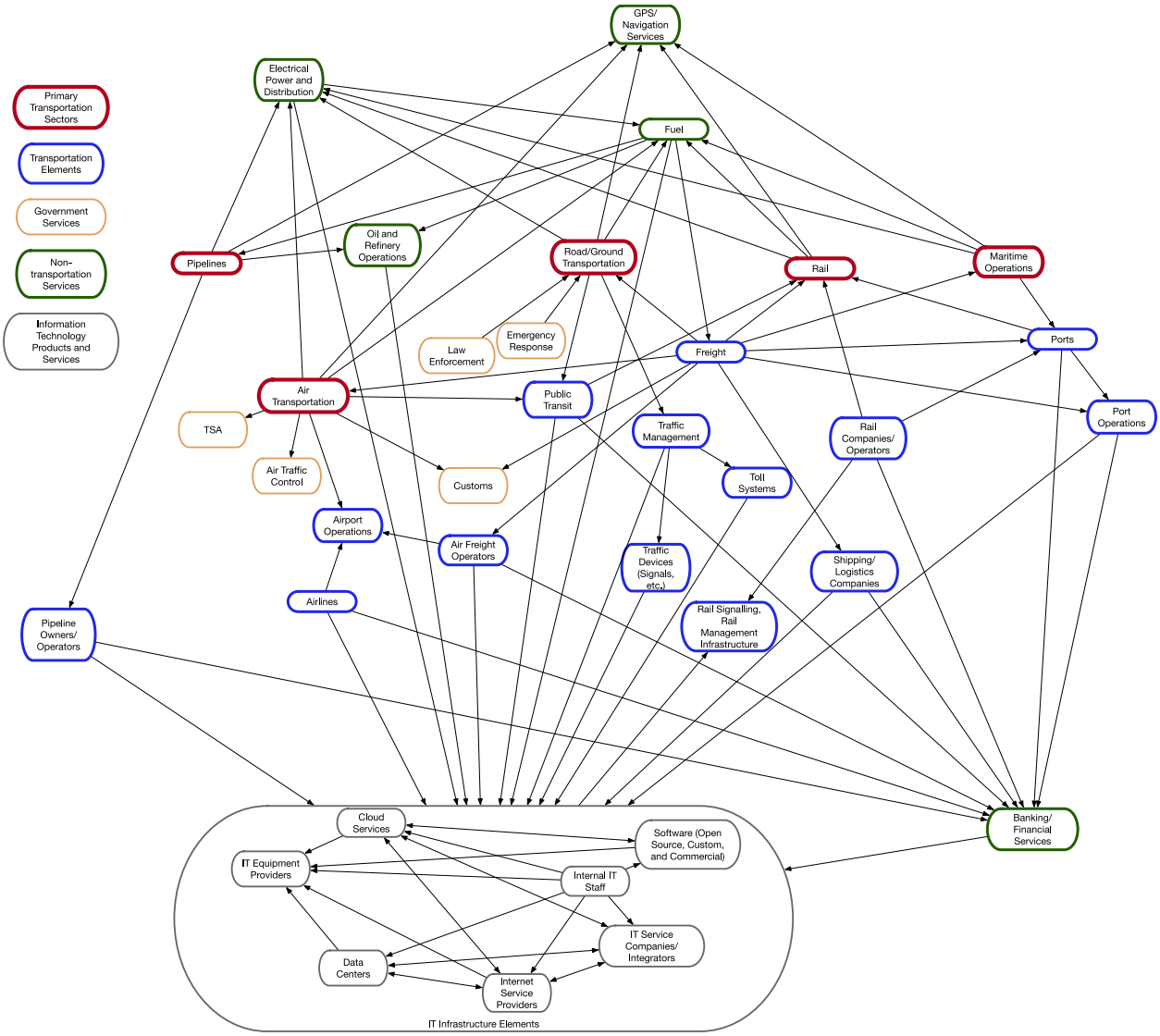

Figure 14 Dependency Diagram (IT Infrastructure Elements)

These IT infrastructure elements, the systems, networks, cloud services, equipment, software, operating systems, internet services, support staff, consultants, companies, and individuals all provide attack vectors for every cyberattack. And every element of the dependency diagram is dependent and connected to these IT infrastructure elements. The attacks on these IT elements have the potential not only to impact any specific transportation service, supporting industry/service, or transportation sector, but to ripple through the entire system often in unexpected ways due to the complex nature of the dependencies that exist in our global economy and transportation systems. Impacts on any primary target can be amplified as they travel through these lines of dependency connection.

A review of some of the case studies presented in this report are illustrative of this principle. The Colonial Pipeline was an attack on the business systems of a single pipeline operator. The impact of the attack resulted in fear for the operation controls of the pipeline, resulting in a shutdown of the pipeline, resulting in fuel delivery shortages, resulting in a lack of fuel

(gasoline, diesel, and aviation fuel) for much of the road/surface and air transportation systems. This in turn impacted air operations, passenger travel, public transportation, and freight deliveries. Even for the short time the pipeline was shutdown, there were substantial transportation and economic impacts.

NotPetya is perhaps the most extreme example of the ripple effect of a cyberattack with significant impacts beyond the original target. What was a state sponsored attack on a foreign government resulted in significant collateral damage to many companies, including multiple transportation sectors, several experiencing multiple hundreds of millions of dollars in damage from the attack. In the case of Maersk, the chain of dependency started with an attack on a family run business providing services and software, a subsequent infection of a single unpatched Maersk workstation upon installation of a software package, to a worldwide infection of the Maersk network and systems. This resulted in the shutdown of Maersk's systems resulting the significant disruption of Maersk shipping operations. The shutdown of Maersk resulted in significant impacts in port operations around the world, disrupted freight distribution around the world, with significant impacts on business in every sector that depends upon freight distribution. Economic and operational impacts on a single small family business spread across the entire world in a matter of hours. Figure 15 illustrates this spread within our dependency diagram. The lines of dependency through which this attack spread are highlighted in yellow. The potential freight consumer sectors impacted are included within the diagram.

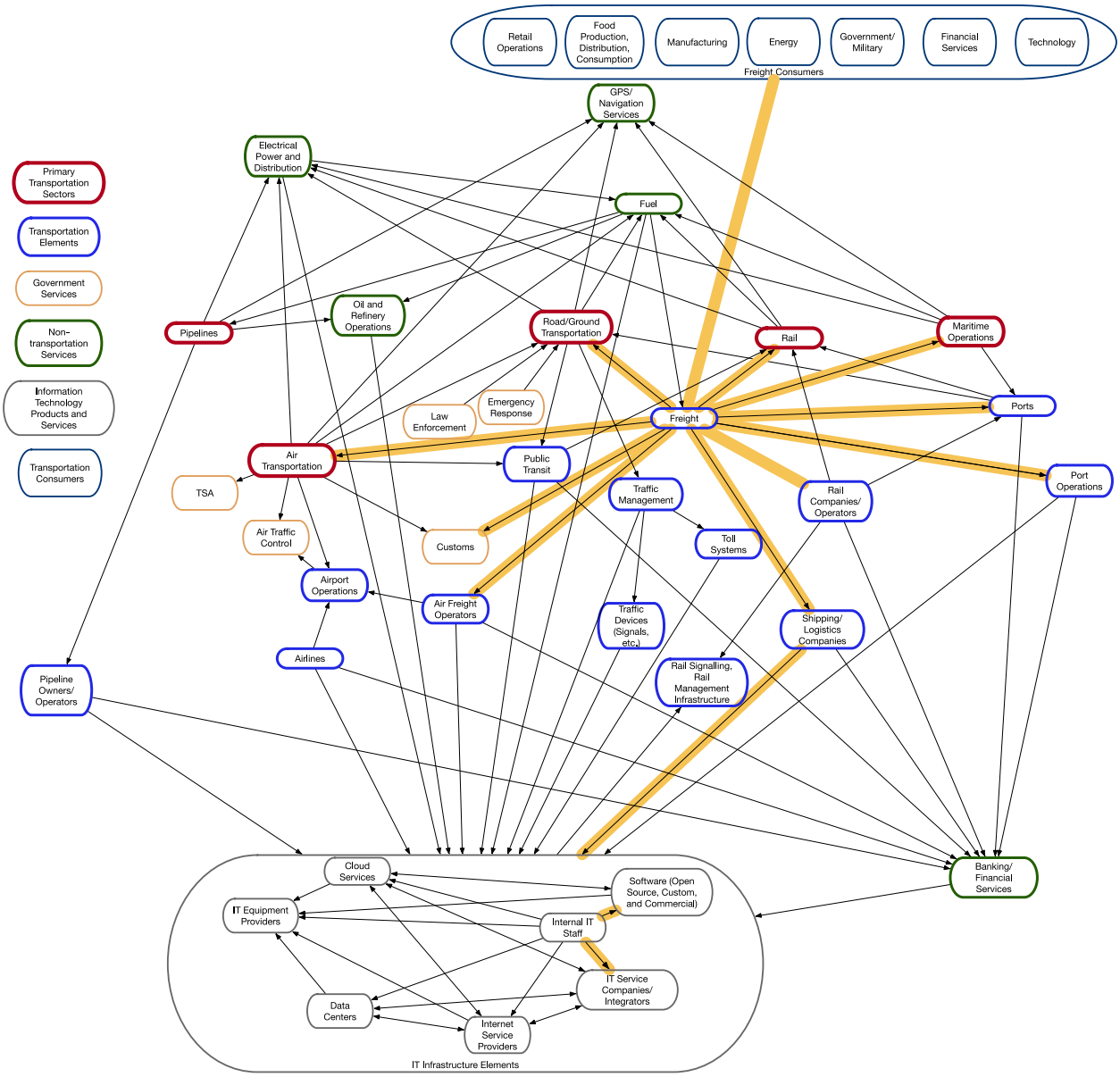

Figure 15 Maersk NotPetya Impacts Dependency Diagram

We can use such dependency diagrams to start to understand how the impacts of an attack can spread and how such impacts can be mitigated by strategies developed to limit the spread of the attack impacts through the system.

The dependency diagram is a very simplistic representation, and many of the elements that are illustrated represent entire industries, large and small business that provide services and products, employees, contractors, users of the systems, all with their own secondary dependencies. Each of these are potential points of entry by a determined hacker. In addition, these dependencies and the complexity of the connections are constantly changing. Our society's digital environment is becoming more complex every day. Still, exploration of such

diagrams is useful to analyze and assign risk and determine priorities and actions for limiting the impact of a successful cyberattack.

6. Actions to Address Our Transportation Systems Cybersecurity Challenges

To counter the threat of cyberattacks on our transportation system, actions are needed at several different levels. Those involved in managing, operating, maintaining, improving, and building our transportation system as well as those using it all have a role to play. The challenge needs to be addressed at multiple levels, including:

- Political
- Economic
- Organizational
- Personal
- Technical

Notice that technical is listed last. Typically, cybersecurity is viewed as primarily a technical challenge. It is not. While technical elements are a critical element of securing our transportation system, many of the most important challenges to address are at the other levels listed; political, economic, organizational, and personal. Leadership and understanding of the threat and needed actions at the highest levels, not only setting cybersecurity as a top priority, but funding it as well is the most critical political need. Organizational leadership, ensuring within our organizations, private and public, that cybersecurity is a top priority and supporting it with funding and support is needed. Ensuring that all individuals understand that their personal actions and vigilance are critical to ensuring security of our infrastructure and data and understanding not only how to avoid a breach, but actions necessary when one occurs are needed at a personal level. Until those are addressed, the technical teams currently addressing the current cyber threats will be unable to secure our transportation system.

This report will discuss actions that can be taken at each level, and specific transportation related issues that create challenges or impediments in each of these specific areas.

6.1. Political

The Colonial Pipeline attack and the national vulnerabilities it exposed resulted in an immediate Federal response to improve cybersecurity of pipelines as well as other critical infrastructure elements. The pipeline shutdown occurred on May 7, 2021, and by May 12, 2021, an Executive Order on Improving the Nation's Cybersecurity was issued by the White House (Joseph R. Biden, 2021).

This executive order provided key political leadership in response to the attack by both prioritizing cybersecurity and prescribing key actions to be taken to address critical cybersecurity shortfalls. Unfortunately, as an executive order it was unable to effectively address any increases in funding for these actions and was limited to federal government

systems, providers, and contracts. However, some key points of the order lay out some key actions that are discussed later in this report at the various levels of action, including:

- Section 1 makes clear at the very beginning that not only is cybersecurity a "top priority", but also that "bold changes and significant investments" are required.
- Section 2 spells out requirements to increase collection, storage and sharing of cybersecurity information as well as collaboration between agencies. It ensures federal contracts are updated to include these requirements, a key enforcement mechanism.
- Section 3 requires the federal government to modernize its cybersecurity approach and spells out the need for best practices, Zero Trust Architectures, reference architectures, and the use of cloud services to improve security practices. Other critical elements required include multi-factor authentication, identification and prioritization of critical data for protection, data encryption, and incident response collaboration frameworks.
- Section 4 details software supply chain protection requirements such as secure development environments, automation, vulnerability checks, software provenance and bill of materials, testing requirements, and controls for critical software and software components.
- Section 5 establishes a Cyber Safety Review board of public and private entities to review and assess significant cyber events, threat activity, vulnerabilities, mitigation activities, and agency responses.
- Section 6 requires a set of standard response elements within a "set of operational procedures (playbook)" for planning, vulnerability assessments, mitigation, and agency cyber responses. Critically it also includes a requirement to update the playbook periodically.
- Section 7 includes actions to improve cyber incident and vulnerability detection with a mandatory endpoint detection and response initiative.
- Section 8 works to improve investigation and remediation actions with improvements to collecting and maintaining logs. Logging requirements and policies dealing with types of information collected, log retention, encryption requirements, verification, and centralized access are stated.

Additional leadership is now needed at the federal level to ensure that these actions are carried out in a timely and effective manner. Specific timelines are clearly delineated within the executive order, primarily with establishing the groundwork and initial planning and many activities will be required as a result of these initial actions. Key to its success will be ensuring follow through at the highest political levels throughout agencies implementing the actions delineated within the executive order.

Additional federal efforts regarding cybersecurity requirements for critical infrastructure are continuing. Following the Colonial Pipeline incident, voluntary cybersecurity guidelines for pipeline operators were replaced with mandatory directives. Similar initiatives were undertaken to update requirements for other critical infrastructure elements as well, such as the Cyber Incident Reporting for Critical Infrastructure Act of 2022 (CIRCIA). Rulemaking for this

legislation has just begun. Federal efforts will need to ensure that the requirements are adequate, kept up to date with the latest technology advances, and provide consistency across agencies to allow those implementing these directives to do so effectively.

California has made some early steps in the political arena, both with its landmark IoT security law SB-327, its California Cybersecurity Integration Center established in 2015, and to a lesser extent with respect to cybersecurity, its California Consumer Privacy Act and California Privacy Rights Act. Little information seems to be available publicly regarding its Cybersecurity Integration Center and its last Twitter tweet seems to be dated December 2020. A Google search does not turn up a specific organization website within the first few pages of search results. Some references to the organization point to the California Department of Technology's website.

California would likely benefit from additional regulation and executive action for state and local agencies similar to that at the federal level. Improvements in cybersecurity defense and system resiliency as well as ensuring not only a strategy of fortress defense but to include critical security elements of organizational change, cybersecurity funding, automation, monitoring, software supply chain defense, fast detection and response, universal two-factor authentication, zero-trust architectures, resilient design, and migration to cloud environments will significantly improve California's cybersecurity posture. Ensuring that a risk management approach, coupled with increased prioritization and attention to cybersecurity and funding for these initiatives are needed to effectively and efficiently implement the state's cybersecurity defenses and response and limit attack impacts.

6.2.Economic

Effective cybersecurity requires both effective risk management and prioritization to ensure resources are spent effectively and efficiently. This assumes sufficient resources to meet the threat are available. Unfortunately, there are significant resource constraints to address the threat, in both human and financial resource levels.

Unfortunately, cybersecurity resources are highly educated and in short supply, making these resources expensive. The National Institute of Standards and Technology reports a global shortage of 2.72 million cybersecurity professionals, over 700,000 job openings, and a total workforce of just under 1.1 million (U.S. Department of Commerce National Institute of Standards and Technology, 2022). The U.S. Bureau of Labor Occupational Employment and Wage Statistics for Information Security Analysts from May 2021 list an annual mean wage of $113,270 with regional variations from $72,610 (Northeast Mississippi nonmetropolitan area) to $150,820 (San Jose, Sunnyvale, Santa Clara, CA) (U.S. Bureau of Labor Statistics, 2021). The shortage of talent and the cost of that talent make improvement in cybersecurity a challenging prospect, especially for government agencies at all levels (local, state, federal) with limited budgets and potentially lower pay rates than comparable private pay rates competing within the same limited talent pool. As governmental entities are often required not only to secure

their own cyber environments, but also often charged with regulating cybersecurity efforts within the public and private sector, this is of particular concern.

Spending on information security and risk management will total $172B in 2022, an 11% increase over the previous year, which was 13% greater than in 2020 (Pratt, 2021). This is one of many estimates of what the world spends on cybersecurity, and these vary widely, likely due to differences in how such spending is categorized, and the source of information used to calculate the totals. However, one consistent element of the differing estimates is that they are indicating that the spend is increasing at a significant pace. Given the increases in the number of attacks and the losses within the average individual attack, this is not surprising. Cybersecurity is receiving additional attention and investment in corporate and government environments, along with increased budgets. Congress increased the budget for the Cybersecurity and Infrastructure Security Agency $300M more than was requested in the recent Cyber Incident Reporting for Critical Infrastructure Act of 2022. Organizations can expect that their cybersecurity and risk management budgets will require significant increases for the foreseeable future to manage risk of attack and limit impacts of successful attacks.

What organizations can and should do is contain these cost increases and prioritize actions to focus on the most successful elements of a cybersecurity strategy. Utilizing investments in cybersecurity to also improve operational effectiveness and resiliency can have positive impacts not only on security, but also on operational effectiveness. Organizations that take a holistic approach to risk management and cybersecurity, view it as a business decision and investment, tailor their risk management strategy to their own specific industry, and maintain cybersecurity expertise and authority at the highest levels of the organization are more likely to have the best results from their cybersecurity expenditure.

Most critically however is that organizations within a critical infrastructure such as transportation, especially those who need to improve their cybersecurity posture, should be looking to improve this posture with potentially significant increases in their IT, cybersecurity, and training budgets. These increases should be coupled with improved risk management practices and prioritization for maximum impact on risk reduction and organizational resiliency.

6.3.Organizational

Perhaps the most critical thing any organization can do, particularly at a senior leadership level, is to understand the following:

Every organization will continue to be attacked and be negatively impacted by those attacks. While you need strong and effective measures against every attack within your IT infrastructure, you cannot successfully defend against every attack. Your weakest points are the people within your organization, and currently nothing you can do will stop 100% of the attacks against your systems and data. Each attack has potential for significant consequences to your organization and the entire transportation system beyond your organization. Even attacks not

directed at your organization or systems can result in such consequences and efforts are likely needed to minimize impacts from secondary damage not directed at your organization.

The organizational actions transportation related entities should take can be thought of in four categories:

- Organizational incentives and priorities
- Organizational structure and leadership
- Workforce preparedness
- Organizational understanding of cybersecurity risk and risk management

6.3.1. Organizational Incentives and Priorities

Organizations' most significant opportunities for improvement in the cybersecurity posture derive from elevating cybersecurity priorities within the organization, with incentivizes for improvements in cybersecurity posture to demonstrate commitment and the importance of cybersecurity to the organization. Demonstrating that cybersecurity is of critical importance to the organization not only with messaging, but with many of the actions included within this report, along with the backing at the highest leadership levels is needed for success. Messaging to all members and all levels of the organization the importance of cybersecurity, the risks of attack, and potential impacts of a successful attack is an effective tool to demonstrating its importance to the organization.

Creating incentives for the organization, particularly for those tasked with implementing cybersecurity within an organizations IT infrastructure further demonstrate the importance of cybersecurity to an organization. Incentives structured to emphasize the use of risk management principles, effective defense mechanisms, improvements in systems resiliency to attack, improvements in attack detection and alerts, system updates and patch improvements, and other known strategies further demonstrate the importance of cybersecurity. Incentives should be structured to incentivize the full range of cybersecurity measures necessary to defend against attack as well as detect, minimize impact, and recover from attack while limiting the expense and operational impacts of a successful attack.

6.3.2. Organizational Structure and Leadership

Organizations should ensure that the organization leadership and structure is constructed to prioritize and execute cybersecurity efforts at the appropriate level. This can be accomplished through:

- Ensuring that there is a specific individual and department/agency responsible for cybersecurity of the organization with appropriate authority, budget, and dedicated staff dictated by appropriate risk assessment and management efforts to address cybersecurity issues.
- Ensuring that the individual responsible for cybersecurity is elevated to the appropriate leadership level within the organization, generally at the C-level. In large organizations,

this is usually a Chief Information Security Officer. Develop support structures for cybersecurity decision making that include operational, financial, executive, human capital, program management, technical, and other critical sectors of an organization that are impacted by and can support cybersecurity priorities and decision making. For transportation related entities and organizations, this may include other stakeholders that support or utilized the transportation system for which the organization is responsible.

- Provide support for sufficient cybersecurity budgets, not only within the dedicated department responsible for cybersecurity, but within other elements of the organization that are necessary to implement cybersecurity programs, systems maintenance, systems resiliency, workforce education, or other cybersecurity related elements. Spending on cybersecurity should be based on risk assessment and business or organizational objectives rather than technical objectives.
- Develop and actively support clear organizational policies regarding cybersecurity. Such policies should be developed for the organization itself and include interactions with agencies, partners, contractors, and others outside of the organization.
- Emphasize cybersecurity skills development as a critical workforce development strategy, especially for those directly responsible for cybersecurity as well as within the IT organization.
- Identify and prioritize cybersecurity elements based on risk management and business needs. Transportation agencies need to consider not only the risk to their own operations, but also risk to dependent societal elements and other transportation system partners. Ensure that leadership at all levels understands the cybersecurity risks, priorities, and actions identified in any risk management and business analysis.
- Emphasize within organizational communications and actions the important role every individual within the organization plays to secure the organization's information systems and data. Ensure such emphasis is placed on communications and actions at all levels of the organization.
- Understand that effective cybersecurity is not only a technical objective but is also an operational objective. Ensuring operations continue by both reducing the likelihood of a successful attack as well as the impact of any successful attack are critical to an organization's operations. Conducting risk assessments and prioritizing cybersecurity related activities should focus on operational risk, impacts, and objectives rather than technically focused objectives. This increases the opportunity for identifying secondary benefits to the organizations operations resulting from cybersecurity activities such as increased operational and system resiliency and reliability.

Organizations need to understand that while risk assessments are critical to develop a cybersecurity strategy, such assessments are easily biased based on a lack of understanding of risk, including, what risks are to be assessed, the amount of risk present, and the level of risk that an organization is willing to assume. This is especially true given the difficulty of addressing risk across multiple operational, business, and technical domains within complex organizations. Adding the complexity of risk from and to external entities such as partners, other agencies,

contractors, and the public typical within the transportation domain, makes an accurate assessment and understanding of risk even more difficult, especially for public agencies. Organizations should consider input for such assessments is gathered from across a broad range of operational units and external entities. External reviews and third-party expert assessments may be beneficial.

6.3.3. Workforce Preparedness

Workforce preparedness to support cybersecurity initiatives is critical to their success. To be effective, initiatives should be developed to ensure the entire workforce is engaged in cybersecurity at the level appropriate to each specific segment of an organization's workforce. Every part of an organization, including every individual that supports its transportation mission, has a role to play in securing an organization's information and cyber assets. As we've seen in the case studies, any individual at any level in the organization can be the key enabler of a successful attack resulting in significant damage to the organization and the transportation system. Providing each individual with education and training to understand their role, recognize a potential attack, take action to avoid such an attack, and report potential attack activity is critical. This may need to be more than a single annual online training course to meet a regulatory or policy requirement. Ensuring the workforce is prepared should include several efforts including:

- Hiring effectively and workforce composition
- Workforce training in basic cybersecurity
- Advanced skills development for key workforce elements responsible for cybersecurity
- Executive and leadership training and education

6.3.3.1. Hiring Effectively and Workforce Composition

Cybersecurity expertise is expensive and public agencies struggle to compete for talent to fill internal positions within the organization. Contracted external resources can fill some of the need, but often come at still higher cost. They can however provide significant benefit in filling critical resource and expertise needs when supplementing efforts to develop or improve cybersecurity programs and critical needs during cybersecurity incidents. Internal resources provide significant benefit, especially in leadership positions that can advocate for resources and provide information for executive management within transportation agencies. Internal resources also provide continuity in effort, which is critical in cybersecurity as it requires continuous analysis and management of risk, monitoring, defense, and ensuring resilience of information systems. Small transportation related companies often have some of the same issues in competing for talent. Even large firms struggle to obtain cybersecurity talent.

To effectively address cybersecurity issues organizations must address the challenge at all levels of the organization: executive leadership, management, and information technology with individuals with an understanding of cybersecurity and its importance to the operations of the

organization. Those in information technology need additional skills related to cybersecurity within their areas of specialization and those dedicated to cybersecurity of the organization require the highest level of cybersecurity skill sets. This requires developing hiring practices that can both identify individuals with the skills necessary and validate their skill level. This may also require organizations to evaluate the need to step outside of normal human resources practices and pay levels to attract such talent, especially to develop a core competence at each level of the organization. Developing a strategy for providing a mix of internal and external resources with provisions for addressing critical time sensitive human capital needs during a cybersecurity incident should be considered. Smaller transportation agencies may benefit from cooperative agreements to share resources.

6.3.3.2. Workforce Training in Basic Cybersecurity

Most large organizations today have implemented basic required cybersecurity training for their workforce, either due to regulatory requirement or organizational policy. Organizations that have not implemented such training should implement training programs. All organizations should evaluate the effectiveness of their training programs and ensure they are both effective and address current security threats, issues, and practices.

6.3.3.3. Advanced Skills Development for Key Workforce Elements Responsible for Cybersecurity

Cybersecurity is a constantly changing field. Targets, attack methods, threat actors, technology, security tools and methods, defense strategies and methods, regulation and policy, institutional risk, assessment methods, and other elements of the cyber landscape are constantly changing. Yesterday's threat environment is not today's and tomorrow's will be different than today's. Not only should basic workforce training change, but skills development of an organization's cybersecurity workforce is critical to ensuring its success. Organizations should develop and implement programs to ensure this critical element of its organization has the skills necessary to manage the organization's cybersecurity risks. This planning should also include other elements of its information technology workforce that implement and maintain the systems that are targets of attacks. This skills development should be part of any risk management practice to ensure funding for cybersecurity related skills development.

6.3.3.4. Executive and leadership training and education

Those responsible for leadership of the cybersecurity efforts within the organization must develop efforts to inform and educate and assist executive leadership and key management elements of their organizations to understand the risks, determine acceptable levels of risk, and identify needed efforts to address the risk. Ensuring that leadership is educated and has an understanding of formal risk management efforts and outcomes, the organization's capabilities through formal capability assessment methods such as the NIST Cybersecurity Framework (National Institute of Standards and Technology, 2022), potential impacts to the business or agency and its operations, and options to address the risks is critical to addressing cybersecurity.

6.3.4. Organizational Understanding of Cybersecurity Risk and Risk Management

Ensuring that those responsible for conducting risk management activities and developing the resulting action and priority options have a clear understanding of the methods used to assign and assess risk and develop effective strategies to mitigate those risks is critical. Organizations should ensure those whose role it is to execute those actions and strategies, identify and respond to attacks, and secure systems and data within the organizations are trained to effectively carry out those tasks understand the current and future state of cybersecurity. Supporting education and active participation in professional cybersecurity organizations for those with responsibility to secure the organization from the impacts of an attack is a way to ensure continued understanding of cybersecurity risk and management of that risk. Improving communication between business operations, information technology, and cybersecurity elements of an organization's workforce will improve the understanding of risk specific to the organization's operations and result in better prioritization of activities to address that risk in a cost-effective manner.

6.4.Personal

The success of every cyberattack depends on personal actions of individuals within a target organization. These attacks usually depend on multiple actions of many individuals, sometimes within multiple organizations to be successful and to broaden their impact. Organizations that combine effective education programs to ensure understanding of this reality by every individual within the organization with effective monitoring tools and programs to detect actions that may or do result in a cyberincident and automatically isolate impacts of such an action will be more successful in their cybersecurity efforts.

6.5.Technical

Many organizations view cybersecurity as the responsibility of the technical elements of the organization. This is flawed. The impacts of poor cybersecurity, while the information technology elements of an organization are not immune, are most critically felt by the organization's ability to conduct its mission. This is particularly true in the most successful attacks. Disruptions to an organization's ability to carry out its mission and responsibilities are primarily experienced by the organization and those it serves, not the organization's information technology department. Costs of attacks and recovery from the attacks are borne by the organization. Lost revenue and reputational damage are borne by the organization. For transportation businesses and agencies, as shown in several case studies within this report, the costs are often borne by the public at large and society.

To address cybersecurity, organizations must take primary responsibility for cybersecurity. However, information technology elements of the organization have a unique and critical role to educate, inform, monitor, defend, and, when an attack is successful, recover from the attack.

6.5.1. Adopt Risk Management Approach, Align with Organizational Objectives

Information technology elements of an organization are often the initiators of the cybersecurity conversation within the organization. They should advocate for a structured approach to cybersecurity that both understands the cybersecurity risks the organization faces, develop strategies to mitigate those risks, and align those risks and mitigations with the organization's mission and objectives. They should actively partner with others within the organization to better understand the operations of the other organizational elements and the organization's financial resources to align cybersecurity costs, risk tolerance, and available funding into multiple funding and prioritized mitigation strategy options. This allows the organization and its executive leadership to control the funding for cybersecurity efforts and level of acceptable risk. Cybersecurity actions should be defined in terms of business objectives rather than technical objectives whenever possible. The effort should be part of the organization's enterprise risk management practice, when one exists. Those without such a practice, with limited experience or success with formal risk management, or those too small for such formality may still benefit and find it cost effective to engage an outside consultant to assist in such an effort.

6.5.2. Conduct Capability Assessment

Information technology elements of an organization should initiate an assessment of the organization's cybersecurity capabilities. This helps identify not only their current capabilities, but also identifies gaps. Coupled with a risk assessment, it also can help prioritize the gaps to be addressed. Using a formal capability assessment framework will help to maximize the effectiveness of such an assessment and increase its credibility. Frameworks designed to assess the cybersecurity capabilities of an organization include the NIST Cybersecurity Framework (National Institute of Standards and Technology, 2022), Cybersecurity Capability Maturity Model (U.S. Department of Energy Office of Cybersecurity, Energy Security, and Emergency Response, 2022), and the Cyber Resilience Review (U.S. Cybersecurity and Infrastructure Security Agency, 2022). Many others exist, within both the public and private sector. Conducting honest assessments can help identify funding shortfalls and with a risk assessment help identify funding needed to implement an organization's prioritized and selected actions to address cybersecurity challenges.

6.5.3. Commitment to Resilience

The most effective cybersecurity strategies assume a successful attack that penetrates the organization's defenses. They do not rely solely on defensive measures to prevent an attack. Their cybersecurity strategies may include, but certainly are not limited to, activities for:

- Monitoring and identification of an attack
- Isolation of an attack to limit it's impacts
- Resilience in systems design to allow continued operations through redundant isolated systems, isolated backups, and automated recovery mechanisms

- Incident management and recovery planning
- Practice and testing of cyber defense and recovery activities

These strategies create organizational and systems resilience to attack, increasing the likelihood that the organization will experience fewer negative impacts to its operations during and immediately after an attack.

6.5.4. Specific Technology Elements to Limit the Likelihood of a Successful Attack and Its Impacts

There are, of course, many fundamental technology related elements of an effective strategy to counter cybersecurity attacks. These elements should be part of any cybersecurity strategy, and significant gaps identified during an organization's capability assessment and risk management activities in these should receive high priority to address and remediate. This is not intended to be a complete list of actions, but rather it highlights some key fundamental elements to any cybersecurity strategy.

6.5.4.1. Information Inventory, Controls, and Policies

Data stores that are not known to the organization cannot be protected. Having an inventory of the data stored within an organization, including the metadata that describes the information stored and its elements, is the most fundamental step to securing that information. Having controls for how information is stored and accessed, disclosure and incident controls, access and distribution controls, and the policies, monitoring, and enforcement mechanisms are necessary elements for effective data and information security.

6.5.4.2. Encryption

Ensuring data is encrypted, especially data identified within organizational policies or regulation that requires encryption, is a fundamental step to ensuring the security and privacy of the data. Controls and protection for encryption keys should not be overlooked, as encryption only protects the data from unauthorized access when the encryption keys are not exposed. Encryption should be applied throughout the data's lifecycle, from data capture, transmission, storage, and removal.

6.5.4.3. Resilient Design

Existing critical systems should be evaluated for resiliency to attack and new critical systems should be designed with resiliency as a design criteria. Resilient design includes elements of distributed architectures, high levels of redundancy, cloud-based deployment and architectures, isolated and off-line data backups, isolated recovery environments, automated backup, deployment, and recovery capabilities, and automated security monitoring and threat isolation. The goal of this resiliency is to be able to operate critical systems during and after an attack, isolating any attack and have sufficient resources to continue critical business

operations at full or reduced capacity. Improving systems resiliency should be a key consideration when addressing cybersecurity issues.

One key element of resilient system design that is often overlooked is external dependencies. Organizations should review both upstream and downstream dependencies when addressing system resiliency.

6.5.4.4. Network Segmentation and Hardening

This is likely the most over relied upon strategy in the cybersecurity arsenal. However, it remains a critical element that should not be overlooked. It is often the first line of defense for many types of attack. However, it will do little to stop many attacks, such as when an attacker has gained valid credentials via a social engineering or phishing attack.

6.5.4.5. Technology Supply Chain Controls

Several of the case studies in this report exploited weak or non-existent supply chain controls. There are currently several types of tools on the market that provide assistance in this area. External attack surface management tools, software composition analysis tools, and threat intelligence tools are recommended technologies to address software supply chain threats (Nunno, Moyer, & Proctor, 2022) (Nunno, Moyer, & Proctor, 2022). Having controls and policies with such tools can provide some protection against such attacks. They should be part of any effective cybersecurity strategy.

6.5.4.6. IT and Security Policies

Having basic IT and security policies are a fundamental foundation for any cybersecurity strategy. Many frameworks exist for these foundational elements.

6.5.4.7. Access Controls

Having effective controls and policies that define access to systems, data, and information are required for any cybersecurity strategy. This includes ensuring correct provisioning of access when new users are added to an organization or system, maintenance of those access privileges over time, and removal of access when it is no longer required by the organization. Multi-factor authentication should be part of any access control strategy.

6.5.4.8. Emergency and Incident Policies, Procedures, and Practices

Having emergency and incident plans with defined policies, detailed procedures, and organizational practices to define, maintain, and execute the plans is a fundamental need of any cybersecurity response. These plans should ensure proper isolation and identification of the threat, response to the threat, recovery, notification, regulatory and legal responses, and identify external resources to be brought in to assist. This may include law enforcement,

contract resources, insurance requirements, or other predefined actions along with escalation procedures and resources.

6.5.4.9. Monitoring

Threats cannot be addressed unless identified. Often a threat may go undetected, only to be activated months or even longer after the initial attack was successful. Monitoring and identification of threats is the first step to addressing an attack.

6.5.4.10. Update and Patch Management

Update and patch management for operating systems and software is one of the most important elements of effective cybersecurity. Many of the case studies in this report were a direct result of unpatched systems. Organizations risk management activities should identify the level of risk in this key area to be assumed and set goals for time thresholds for system updates accordingly.

This page left blank intentionally

7. Conclusion – Addressing Transportation Challenges to Effective Cybersecurity Action

As part of a designated critical infrastructure of our society, organizations within the transportation industry, public and private, have a unique responsibility to mitigate the impacts of a cyberattack. There are unique and critical dependencies, both within the transportation sector and within the elements of our economy and society that support and use the transportation system. Past attacks demonstrate that a successful cyberattack on any organization within the transportation system or on an organization upon which the transportation system depends (such as IT or financial services, software providers, and equipment manufacturers) can have catastrophic impacts not only on the target organization, but on society and our economic system. As a result, risk management activities must take these broader risks into account, especially within public agencies that serve not a corporate interest, but rather the public and society itself. This is a complicating factor, especially when addressing these issues within the confines of limited public budgets.

7.1. Transportation Industry Cyber Challenges

Transportation also faces challenges with the vast array of equipment and systems with lifecycles often measured in decades. This creates an extremely difficult challenge given what is often a high cost of replacement, limited options to update or patch firmware and software, integration challenges that limit upgrade options, and even developing and maintaining accurate inventories of equipment.

The limited ability to physically secure connected devices in the field creates a multitude of opportunities for cyberattacks. Physical security of connected devices in the field are often limited to a padlocked equipment cabinet with no ability to monitor access.

Public agencies access to the talent required to execute an effective cybersecurity program is extremely limited given the limited talent pool available, high cost of such talent, and limited public budgets and pay scales.

Cybersecurity capabilities are often limited and immature within many transportation agencies. Many of these agencies have not focused on cybersecurity as it was never considered a significant risk, had few advocates within the organization at the levels necessary to demonstrate the need to address the challenge and advocate for funding to address the issue, or simply didn't have the funding necessary to address the challenge. Some organizations, especially smaller organizations, simply have not had the knowledge required to understand or mitigate the risks associated with an attack.

Transportation is undergoing a transition from a physical domain to a cyber-physical domain. Increasingly complex systems are managing the transportation infrastructure, automation is

increasing in both control elements and various types of vehicles, and there is increasing connectivity between the transportation infrastructure elements and the vehicles, ships, and aircraft that use that infrastructure. This added complexity increases the attack surface, increases the opportunity for new attack vectors and methods, and creates a likelihood for more damaging impacts from a successful attack.

The lack of knowledge of the risk of an attack, the risk to an organization's ability to carry out its mission, the risk to society and the public, including public safety, and the actions needed to address the risk are often most evident when new systems and projects are funded, developed, and deployed. There is significant pressure on any project to deliver desired functionality, with cybersecurity likely to be an afterthought. In general, functionality, budget, and project schedule trump any cybersecurity concerns in most transportation projects. This is not unique to transportation. However, it complicates the task of hardening and increasing the resilience of our transportation system by adding new vulnerabilities while we increase the complexity, connectivity, and dependencies within our transportation system.

These challenges and the continued increase in number and complexity of attacks make the change to a more intentioned focus to improve our cyber defense and resilience activities even more of an imperative. Transportation organizations need to prioritize cybersecurity and resilience to attack using risk management and capability assessment, along with the leadership and funding necessary to manage the risk to their operations and society. Without such a shift, organizations risk not only their own operations and financial stability, but those of their customers and those they serve, partners, as well as public safety.

7.2.A Web of Dependencies

Our transportation system is an integral part of our society, critical to our supply chains, energy system, manufacturing capabilities, economic system., and ability travel and function. Every major industry depends on our transportation system. Even our transportation system itself has its own internal dependencies. Understanding these dependencies is critical when defending against cyberattacks and must be accounted for when understanding the risk to an organization and its operations. These dependencies must be identified and understood to effectively define and prioritize cyber defense actions implemented within an organization.

7.3.Recommendations

Defending against and limiting the impact of cyberattacks is a complicated endeavor. It is very attractive to look for tools and prescriptive solutions to the problem, for which there is no shortage within the market. It is also very attractive to ignore or minimize the risk, thinking that it won't happen to you or your organization. However, this is naïve. Templates and prescriptive solutions and industry or government guidelines are often obsolete and provide limited benefit. Both the threats and efforts to counter those threats change too quickly to rely solely upon such guidelines. Many of the suggestions within this report suffer the same issues.

This means that organizations must be more agile. To do this, cybersecurity must be an ongoing and continuous effort with dedicated and sufficient resources to address the challenge. Cybersecurity needs a dedicated team to understand the changing threat and new responses to that threat.

Section 6 provides a number of specific recommendations for organizations to address their cybersecurity risk and reduce the impacts of a successful attack. Most important of these are:

1. Understand that you are already being attacked, and you will be impacted my successful attacks.
2. Commit dedicated human capital and provide them sufficient resources for cybersecurity.
3. Conduct a capability assessment of your organization to quantify the organization's ability to identify, defend against, isolate, and recover from cyberattacks.
4. Develop a continuous risk assessment practice that includes risks to the organization's mission, operations, customers, partners, and in the case of public agencies, the public, society, and public safety. Make sure to identify risks to entities that depend upon the transportation service being provided.
5. Make the case for resources and priorities based upon risk assessment outcomes, specifying risk and impact based upon an organizations mission, operations, and objectives as well as those it serves.
6. Acknowledge and resource efforts that are outside of the dedicated cybersecurity resources such as patch management, network configuration and deployments, application security, cybersecurity training, and other tasks that directly impact the cybersecurity of the organization but may be tasked to other elements of an organization.

Any remaining recommendations and additional actions will generally follow if these six key recommendations are addressed.

This page left blank intentionally

8. Bibliography

A.P. Moller - Maersk. (2018). *2017 Annual Report.* Retrieved from Maersk: https://investor.maersk.com/system/files-encrypted/nasdaq_kms/assets/2018/04/25/13-00-21/A.P._Moller_-_Maersk_Annual_Report_2017.pdf

Belcher, JD, MPP, S., Belcher, T., Greenwald, JD, E., & Thomas, MBA, B. (2020). *Is the Transit Industry Prepared for the Cyber Revolution? Policy Recommendations to Enhance Surface Transit Cyber Preparedness.* San Jose, CA: MINETA TRANSPORTATION INSTITUTE.

Bing, C. (2016, Novembe 28). *Malware targeting San Francisco transit may have been in wild at least 2 months, research shows*. Retrieved from Cyberscoop Transportation: https://www.cyberscoop.com/malware-targeting-san-francisco-transit-may-wild-least-2-months-researcher-says/

Burgess, M. (2022, June 12). *Conti's Attack Against Costa Rica Sparks a New Ransomware Era*. Retrieved from Wired: https://www.wired.com/story/costa-rica-ransomware-conti/

Canales, I. J. (2021, April 15). *The US is readying sanctions against Russia over the SolarWinds cyber attack. Here's a simple explanation of how the massive hack happened and why it's such a big deal*. Retrieved from Business Insider: https://www.businessinsider.com/solarwinds-hack-explained-government-agencies-cyber-security-2020-12

Capano, D. E. (2021, September 30). *Throwback Attack: How NotPetya accidentally took down global shipping giant Maersk*. Retrieved from Industrial Security Pulse: https://www.industrialcybersecuritypulse.com/threats-vulnerabilities/throwback-attack-how-notpetya-accidentally-took-down-global-shipping-giant-maersk/

Center for Strategic and International Studies. (2022). *Significant Cyber Incidents Since 2006.* Washington, D.C.: Center for Strategic and International Studies.

Check Point Research. (2022, March 10). *Leaks of Conti Ransomware Group Paint Picture of a Surprisingly Normal Tech Start-Up… Sort Of*. Retrieved from Check Point Research cp<r>: https://research.checkpoint.com/2022/leaks-of-conti-ransomware-group-paint-picture-of-a-surprisingly-normal-tech-start-up-sort-of/

Checkpoint Software. (2021). *Cyber Attack Trends Mid Year Report 2021.* Tel Aviv, Israel: Checkpoint Research.

Checkpoint Software. (2022). *Checkpoint 2022 Security Report*. Retrieved from Checkpoint.com: https://go.checkpoint.com/security-report/page-global-malware-statistics.php

Federal Bureau of Investigation Interent Crime Complaint Center. (2022). *Internet Crime Report 2021.* Washington, D.C.: Federal Bureau of Investigation.

Federal Bureau of Investigation Internet Crime Complaint Center. (2021). *Internet Crime Report 2020.* Washington, D.C.: Federal Bureau of Investigation.

Freiherr, G. (2021, February). *Will Your Airliner Get Hacked?* Retrieved from Smithsonian Magazine, Air and Space Magazine: https://www.smithsonianmag.com/air-space-magazine/will-your-airliner-get-hacked-180976752/

Greenberg, A. (2018, August 22). *The Untold Story of NotPetya, the Most DevastatingCyberattack in History*. Retrieved from Wired:

https://www.wired.com/story/notpetya-cyberattack-ukraine-russia-code-crashed-the-world/

Greig, J. (2021, July 29). *Hackers used never-before-seen wiper in recent attack on Iranian train system*. Retrieved from ZDNet: https://www.zdnet.com/article/hackers-used-never-before-seen-wiper-in-recent-attack-on-iranian-train-system-report/

IBM. (2020). *Data Breach Report 2020.* New York, New York: IBM.

IBM. (2021). *Data Breach Report 2021.* Armonk, NY: IBM.

Identity Theft Resource Center. (2022). *2021 in Review Data Breach Annual Report.* El Cajon, CA: Identity Theft Resource Center.

Joseph R. Biden, J. (2021, May 12). Executive Order on Improving the Nation's Cybersecurity. The White House, Washington, D.C., United States of America.

Karahalios, H. (2020). Appraisal of a Ship's Cybersecurity efficiency: the case of piracy. *Journal of Transportation Security*, 179-201.

Kempner, M. (2021, May 10). *Things to know about Atlanta's Colonial Pipeline, hit by ransomware*. Retrieved from The Atlanta Journal-Constitution: https://www.ajc.com/news/heres-a-primer-on-atlantas-colonial-pipeline-hit-by-ransomware/TZ2U3EM6RBAQHEAMVO3UYUQHMI/

Madej, P. (2020, August 28). *Malware Attack Hits Philadelphia Transit Worker Data*. Retrieved from Governing: https://www.governing.com/security/malware-attack-hits-philadelphia-transit-worker-data.html

MIGOYA, T. C. (2019, February 21). *https://www.denverpost.com/2018/02/21/samsam-virus-ransomware-cdot/*. Retrieved from The Denver Post: SamSam virus demands bitcoin from CDOT, state shuts down 2,000 computers

National Institute of Standards and Technology. (2022, December 1). *NIST Cybersecurity Framework*. Retrieved from National Institute of Standards and Technology: https://www.nist.gov/cyberframework

Nunno, T., Moyer, K., & Proctor, P. (2022, October 17). *IT for Sustainable Growth: Insights From the 2022 Gartner IT Symposium/Xpo Keynote*. Retrieved from Gartner: https://www.gartner.com/document/4019998?ref=solrAll&refval=344396624

Pratt, M. K. (2021, December 20). *Cybersecurity spending trends for 2022: Investing in the future*. Retrieved from CSO: https://www.csoonline.com/article/3645091/cybersecurity-spending-trends-for-2022-investing-in-the-future.html

Rashbaum, C. G. (2021, June 2). *The M.T.A. Is Breached by Hackers as Cyberattacks Surge*. Retrieved from New York Times: https://www.nytimes.com/2021/06/02/nyregion/mta-cyber-attack.html

SecureLink. (2021, July 8). *Back to Basics: A Deeper Look at the Colonial Pipeline Hack*. Retrieved from Government Technology: https://www.govtech.com/sponsored/back-to-basics-a-deeper-look-at-the-colonial-pipeline-hack

Security Magazine. (2022, February 28). *Ransomware attacks nearly doubled in 2021*. Retrieved from Security Magazine: https://www.securitymagazine.com/articles/97166-ransomware-attacks-nearly-doubled-in-2021

Shaffer, A. (2022, June 6). *The U.S. isn't getting ahead ofthe cyber threat, experts say.* Retrieved from Washington Post: https://www.washingtonpost.com/politics/2022/06/06/us-isnt-getting-ahead-cyber-threat-experts-say/

Tam, K., & Jones, K. D. (2018). *Maritime cybersecurity policy: the scope and impact of evolving technology on international shipping.* Journal of Cyber Policy,.

The Associated Press. (2021, October 27). *NPR KQED*. Retrieved from A cyberattack paralyzed every gas station in Iran: https://www.npr.org/2021/10/27/1049566231/irans-president-says-cyberattack-was-meant-to-create-disorder-at-gas-pumps

The Guardian. (2021, July 11). *'Cyber-attack' hits Iran's transport ministry and railways*. Retrieved from The Guardian: https://www.theguardian.com/world/2021/jul/11/cyber-attack-hits-irans-transport-ministry-and-railways

The Maritime Executive. (2021, November 3). *Cyberattack Hits Multiple Greek Shipping Firms*. Retrieved from The Maritime Executive: https://www.maritime-executive.com/article/cyberattack-hits-multiple-greek-shipping-firms

U.K. National Cyber Security Centre. (2020, May 19). *NCSC statement: EasyJet cyber incident*. Retrieved from National Cyber Security Centre: https://www.ncsc.gov.uk/news/easyjet-incident

U.S. Bureau of Labor Statistics. (2021, May). *Occupational Employment and Wages, May 2021*. Retrieved from U.S. Bureau of Labor Statistics Occupational Employment and Wage Statistics : https://www.bls.gov/oes/current/oes151212.htm#ind

U.S. Cybersecurity and Infrastructure Security Agency. (2022, December 1). *Assessments: Cyber Resilience Review (CRR)* . Retrieved from Cybersecurity and Infrastructure Security Agency: https://www.cisa.gov/uscert/resources/assessments

U.S. Department of Commerce National Institute of Standards and Technology. (2022). Cybersecurity Workforce Demand. Washington, DC, United States.

U.S. Department of Energy Office of Cybersecurity, Energy Security, and Emergency Response. (2022, December 1). *Cybersecurity Capability Maturity Model (C2M2)*. Retrieved from Office of Cybersecurity, Energy Security, and Emergency Response: https://www.energy.gov/ceser/cybersecurity-capability-maturity-model-c2m2

U.S. Department of Transportation. (2019, January 28). *Intelligent Transportation Systems Joint Program Office*. Retrieved from Colorado DOT offers lessons learned after recovering from two 2018 ransomware attacks.: https://www.itskrs.its.dot.gov/its/benecost.nsf/ID/182bf1869996a8578525838c0070b645

Washington Post Staff. (2021, April 22). *The Cybersecurity 202 Network:/.* Retrieved from Washington Post: https://www.washingtonpost.com/politics/2021/02/23/cybersecurity-202-network/?itid=lk_inline_manual_14

Zetter, K. (2020, December 24). *SOLARWINDS HACK INFECTED CRITICAL INFRASTRUCTURE, INCLUDING POWER INDUSTRY*. Retrieved from theintercept.com: https://theintercept.com/2020/12/24/solarwinds-hack-power-infrastructure/

This page left blank intentionally