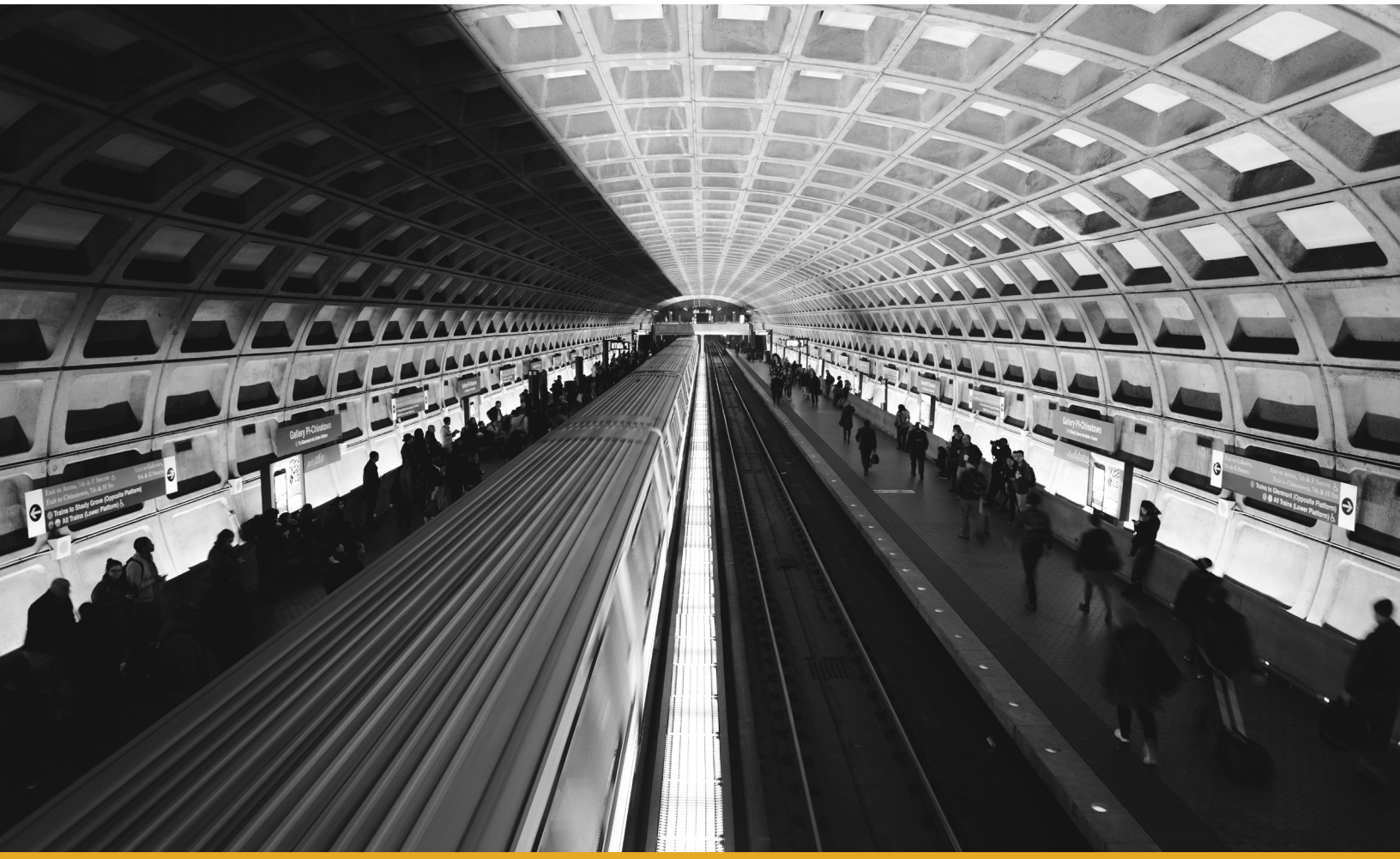
SJSU SAN JOSÉ STATE UNIVERSITY

MTI MINETA TRANSPORTATION INSTITUTE

Is the Transit Industry Prepared for the Cyber Revolution? Policy Recommendations to Enhance Surface Transit Cyber Preparedness

Scott Belcher, JD, MPP
Terri Belcher
Eric Greenwald, JD
Brandon Thomas, MBA



MINETA TRANSPORTATION INSTITUTE

LEAD UNIVERSITY OF

Mineta Consortium for Transportation Mobility

Founded in 1991, the Mineta Transportation Institute (MTI), an organized research and training unit in partnership with the Lucas College and Graduate School of Business at San José State University (SJSU), increases mobility for all by improving the safety, efficiency, accessibility, and convenience of our nation's transportation system. Through research, education, workforce development, and technology transfer, we help create a connected world. MTI leads the four-university Mineta Consortium for Transportation Mobility, a Tier 1 University Transportation Center funded by the U.S. Department of Transportation's Office of the Assistant Secretary for Research and Technology (OST-R), the California Department of Transportation (Caltrans), and by private grants and donations.

MTI's transportation policy work is centered on three primary responsibilities:

Research

MTI works to provide policy-oriented research for all levels of government and the p rivate sector to foster the development of optimum surface transportation systems. Research areas include: bicycle and pedestrian issues; financing public and private sector transportation improvements; intermodal connectivity and integration; safety and security of transportation systems; sustainability of transportation systems; transportation / land use / environment; and transportation planning and policy development. Certified Research Associates conduct the research. Certification requires an advanced degree, generally a Ph.D., a record of academic publications, and professional references. Research projects culminate in a peer-reviewed publication, available on TransWeb, the MTI website (http://transweb.sjsu.edu).

Education

The Institute supports education programs for students seeking a career in the development and operation of surface transportation systems. MTI, through San José State University, offers an AACSB-accredited Master of Science in Transportation Management and graduate certificates in Transportation Management, Transportation Security, and High-Speed Rail Management that serve to prepare the nation's transportation managers for the 21st century. With the active assistance of the California Department of Transportation (Caltrans), MTI delivers its classes over a state-of-the-art videoconference network throughout the state of California and via webcasting beyond, allowing working transportation professionals to pursue an advanced degree regardless of their location. To meet the needs of employers seeking a diverse workforce, MTI's education program promotes enrollment to under-represented groups.

Information and Technology Transfer

MTI utilizes a diverse array of dissemination methods and media to ensure research results reach those responsible for managing change. These methods include publication, seminars, workshops, websites, social media, webinars, and other technology transfer mechanisms. Additionally, MTI promotes the availability of completed research to professional organizations and journals and works to integrate the research findings into the graduate education program. MTI's extensive collection of transportation- related publications is integrated into San José State University's world-class Martin Luther King, Jr. Library.

REPORT 20-36

IS THE TRANSIT INDUSTRY PREPARED FOR THE CYBER REVOLUTION?

POLICY RECOMMENDATIONS TO ENHANCE SURFACE TRANSIT CYBER PREPAREDNESS

Scott Belcher, JD, MPP
Terri Belcher
Eric Greenwald, JD
Brandon Thomas, MBA

September 2020

A publication of
Mineta Transportation Institute
Created by Congress in 1991

College of Business
San José State University
San José, CA 95192-0219

TECHNICAL REPORT DOCUMENTATION PAGE

1. Report No. 20-36	2. Government Accession No.	3. Recipient's Catalog No.
4. Title and Subtitle Is the Transit Industry Prepared for the Cyber Revolution? Policy Recommendations to Enhance Surface Transit Cyber Preparedness		5. Report Date September 2020 6. Performing Organization Code
7. Authors Scott Belcher, JD, MPP, https://orcid.org/0000-0003-3147-4041 Terri Belcher, https://orcid.org/0000-0002-9355-4357 Eric Greenwald, JD, https://orcid.org/0000-0002-3225-6890 Brandon Thomas, MBA, https://orcid.org/0000-0002-7986-2716		8. Performing Organization Report CA-MTI-1939
9. Performing Organization Name and Address Mineta Transportation Institute College of Business San José State University San José, CA 95192-0219		10. Work Unit No. 11. Contract or Grant No. 69A3551747127
12. Sponsoring Agency Name and Address U.S. Department of Transportation Office of the Assistant Secretary for Research and Technology University Transportation Centers Program 1200 New Jersey Avenue, SE Washington, DC 20590		13. Type of Report and Period Covered Final Report 14. Sponsoring Agency Code
15. Supplemental Notes DOI: 10.31979/mti.2020.1939		

16. Abstract

The intent of this study is to assess the readiness, resourcing, and structure of public transit agencies to identify, protect from, detect, respond to, and recover from cybersecurity vulnerabilities and threats. Given the multitude of connected devices already in use by the transit industry and the vast amount of data generated (with more coming online soon), the transit industry is vulnerable to malicious cyber-attack and other cybersecurity-related threats. This study reviews the state of best cybersecurity practices in public surface transit; outlines U.S. public surface transit operators' cybersecurity operations; assesses U.S. policy on cybersecurity in public surface transportation; and provides policy recommendations that address gaps or identify issues for Congress, the Executive Branch, and the public surface transit agencies. Research methods include an online survey of public surface transit professionals in the United States and oral interviews conducted with members of the Executive Branch (e.g., U.S. Department of Transportation, U.S. Department of Homeland Security, The White House, and others), as well as research of literature published in periodicals.

17. Key Words Cybersecurity, policy, safety, security, transit	18. Distribution Statement No restrictions. This document is available to the public through The National Technical Information Service, Springfield, VA 22161		
19. Security Classif. (of this report) Unclassified	20. Security Classif. (of this page) Unclassified	21. No. of Pages 87	22. Price

Form DOT F 1700.7 (8-72)

DOI: 10.31979/mti.2020.1939

Mineta Transportation Institute
College of Business
San José State University
San José, CA 95192-0219

Tel: (408) 924-7560
Fax: (408) 924-7565
Email: mineta-institute@sjsu.edu

transweb.sjsu.edu

092720

ACKNOWLEDGMENTS

The authors thank the following people for their important contributions to this project:

- Paul Skoutelas, President and CEO of the American Public Transportation Association (APTA), and the rest of the APTA team for their ongoing support and guidance;

- Polly Hanson, Senior Director of Security, Risk and Emergency Management, APTA, for her tenacious advocacy and sage advice;

- Ed Merlis for his early support in framing the study and the legislative framework and editing;

- Editing Press for editorial services; and

- MTI staff, including Executive Director Karen Philbrick, PhD; Deputy Executive Director Hilary Nixon, PhD; Graphic Designer Alverina Eka Weinardy; and Communications and Operations Manager Irma Garcia.

TABLE OF CONTENTS

LIST OF FIGURES

LIST OF TABLES

EXECUTIVE SUMMARY

Information abounds to support public transit agencies in developing their own cybersecurity preparedness programs; however, few prescriptions exist. Most available resources are general in nature or have been adapted from other industries. Effort is required to bring these general resources into conformity with a particular agency's needs, given its unique status and set of circumstances. In the authors' assessment, there is a reasonable amount of useful and effective information available to assist transit agencies in implementing a cybersecurity program: for instance, using the National Institute of Standards and Technology (NIST) cybersecurity framework and implementation guides from the federal government, the American Public Transportation Association (APTA), and others. However, despite these resources, far too many agencies have not implemented adequate cybersecurity measures and are ill prepared to respond to a cyber incident.

For this report, the authors conducted a digital survey to understand each agency's level of cybersecurity preparedness, along with dozens of in-person interviews. The most startling statistic to come from this work is that over 70% of the agencies that responded to the survey claim they have not yet had many (or any) cybersecurity incidents. Data and research from other industries suggests that this statistic should be inverted, whereby a large majority of organizations experience cybersecurity incidents on an increasing and consistent basis. Is public transit really different from other industries, or are incidents occurring but not being identified or reported?

The problem may be that cybersecurity is not yet widely seen as a critical issue among public transit leadership. The incidents that have happened have not spurred the action one would expect. Both reporting and accountability of them are murky given the current regulatory environment. There is an exponentially expanding gap between the cybersecurity preparedness that should exist and the growing exposure to threats from increased reliance on technology and the opportunity for access by malicious actors.

The report concludes with a series of policy recommendations intended to engage the Executive Branch, legislative actors and industry to find ways to continue to educate and direct agency leadership towards the need for action.

I. INTRODUCTION

San Francisco's Bay Area Rapid Transit (BART) serves a population of 3.3 million people and has operating expenses that exceed $650 million a year, ranking it as one of the top 15 largest public transit agencies in the U.S.[1] Given its size, BART has access to the Department of Homeland Security's Cybersecurity Advisor's program (which focuses on the largest U.S. transit agencies). BART has both the resources and the focus to be more effective than many other transit agencies at cybersecurity preparedness.

In 2017, a few fresh faces from outside the transit industry were brought aboard to augment BART's cybersecurity program. One initiative driven by this new team was a process of due diligence to verify the pedigree of all newly deployed hardware elements that were part of its capital projects. The Silicon Valley Berryessa Extension (SVBX) was one of the projects under review. In March 2018, testing was set to begin for BART to accept the handover of the contractor's work on the extension. This contractor is one of the larger, more respected contractors in the industry. Trust was strong.

The new team asked for the make, model, and serial numbers for the hardware suite that included over 1,000 devices supplied by Cisco, one of the largest and most prestigious networking hardware manufacturers in the United States. Cisco takes great care in managing its supply chain, tracking by serial number when a device is manufactured, when it is put into service, who owns it over time, and—most importantly—when it is decommissioned. This supply chain data proved to be invaluable for BART.

Because its size and annual spend, BART enjoys a close relationship with Cisco. Even with this close relationship, however, the trusted contractor in the middle introduced a significant issue into BART's cybersecurity channel. Through this due diligence and working relationship with Cisco, BART discovered that 86% of the serial numbers on the Cisco devices turned out to have been decommissioned in hostile nations in years past. Further research discovered hidden backdoors on the devices, as well as a persistent 'ping' where data are sent to a foreign nation hostile to American interests. In short, BART discovered intentionally planted spyware.

Fortunately for BART, given its relationship with Cisco, replacements for these 1,000 devices were shipped within 72 hours, and BART's team scrambled to install the replacements within 10 days of discovery. However, given the role these devices play in BART's network, the vulnerability, had it been exploited, could have been swift and severe. Law enforcement, including the local Sheriff's office, the Federal Bureau of Investigation (FBI), and the U.S. Department of Transportation's (U.S. DOT) Inspector General's office are still at work pulling the threads and looking to hold those responsible for this attack accountable. This investigation is impacting many transit operators in other cities well outside the confines of the San Francisco Bay Area that did business with the same contractor and subcontractor that unwittingly purchased counterfeit hardware and have now been swept into an international criminal investigation.[2]

PUBLIC TRANSPORTATION OVERVIEW

Public transportation is deeply woven into American society and is by its very definition accessible to all. For people who rely on it daily, public transit is critically important. Public transportation includes urban or rural bus systems, paratransit, bus-rapid transit (BRT), water-borne services, subways, light rail, streetcars and other urban rail networks, and passenger rail (Figure 1).

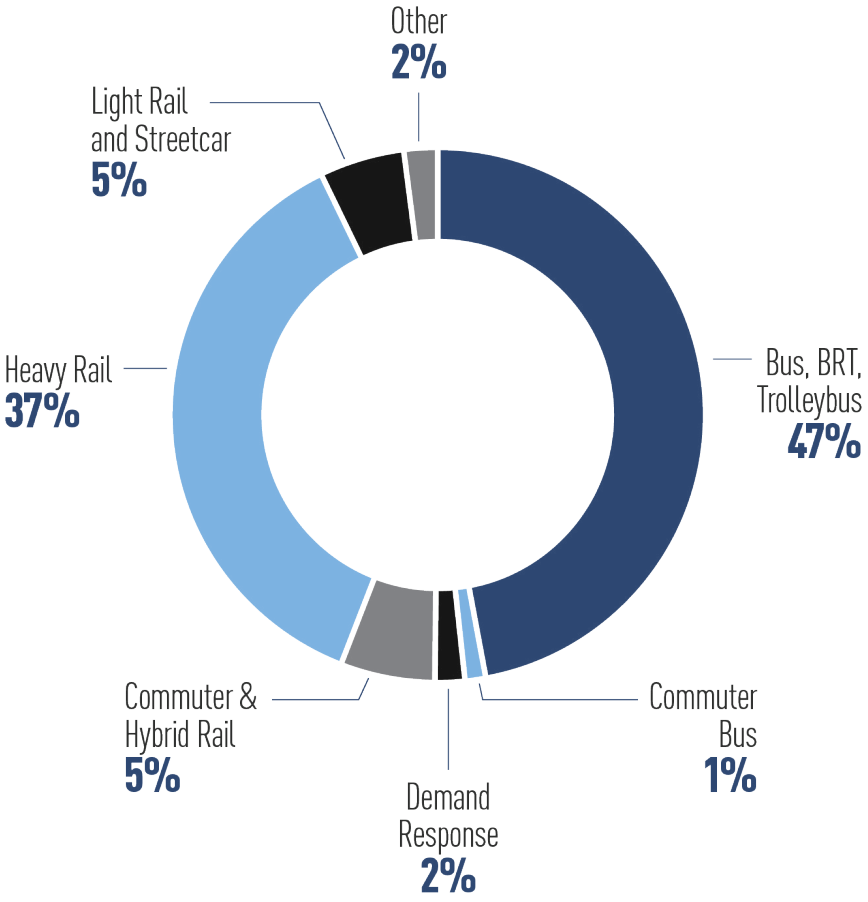
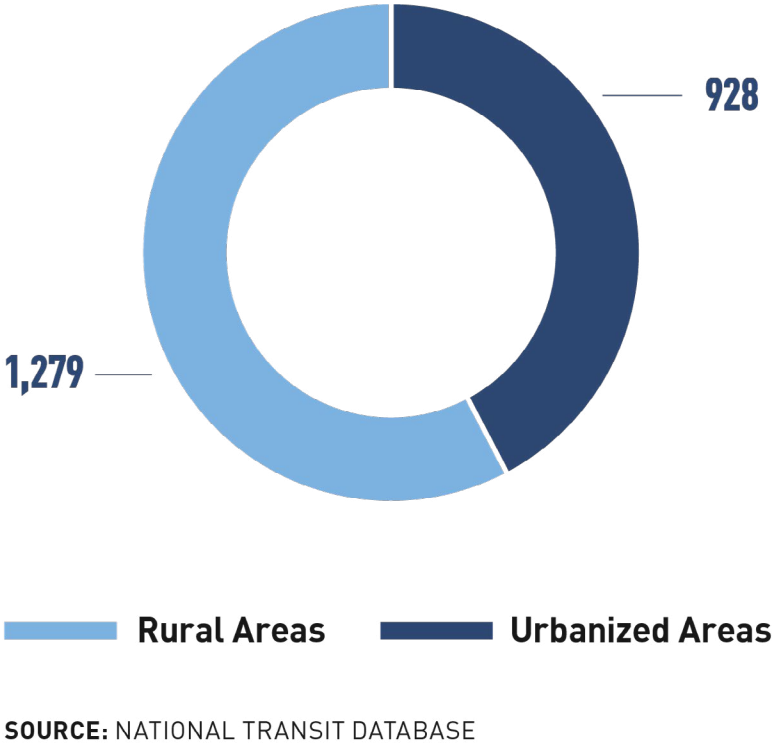


Figure 1. Share of Unlinked Passenger Trips by Mode, 2018[3]

Public transportation is available in every state. In its *2020 Public Transportation Fact Book*, the American Public Transportation Association (APTA) reports that approximately 6,800 organizations provide public transportation through the variety of modes outlined in Figure 1.[4] Of this total, an estimated 4,580 are public nonprofit providers. Systems operating in urbanized and rural areas that receive grant money from the Federal Transit Administration's (FTA) Urbanized Area Formula Program (5,307) or Rural Formula Program (5,311) are required to report to the National Transit Database (NTD) as full, reduced, or rural systems. The NTD is the primary source for information and statistics on transit systems in the United States. Congress requires the NTD to collect financial and service information annually from public transportation agencies that receive benefits from FTA grants.[5] Of the 2,207 NTD reporting transit systems in 2018, 1,279 were in rural areas and 928 were in urbanized areas (Figure 2).

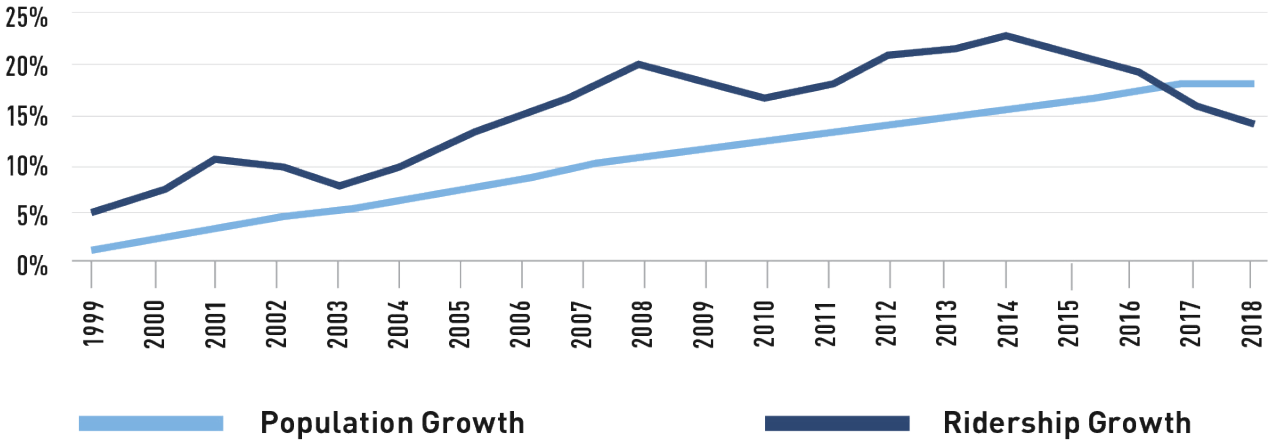


SOURCE: NATIONAL TRANSIT DATABASE

Figure 2. Number of NTD Reporting Transit Systems[6]

Although rural transit providers make up 58% of the NTD reporting systems, they only provide approximately 1% of the total unlinked trips taken.[7] These are important trips, however, because they are often the only means of transportation for vulnerable populations.

"Importantly, since the early 1970s, public transportation has shown a long-term growth in ridership, with approximately 37% more unlinked passenger trips taken in 2018."[8] Public transportation provided 9.95 billion unlinked passenger trips in 2018. Until 2017, the rate of transit ridership growth exceeded the rate of population growth (Figure 3).



SOURCE: APTA FACT BOOK ANALYSIS AND U.S. CENSUS BUREAU

Figure 3. Population vs. Ridership Growth Since 1998[9]

With this growth in transit usage comes a growth in security risks to transit systems—including risks from cybersecurity vulnerabilities. As more systems and resources are digitized and connected, more opportunities arise for malicious actors and system malfunctions to disrupt operations on a massive and potentially catastrophic scale.

APTA, the primary trade association for the public transit industry, made cybersecurity a priority issue more than a decade ago with the issuance of the APTA Recommended Practice entitled *Securing Control and Communications Systems in Transit Environments*, *Part 1*[10] and it has followed that up with subsequent guidance over the years. In an interview upon becoming the Chair of the APTA Board in 2018, Nathaniel P. Ford, Sr. Chief Executive Officer of the Jacksonville Transportation Authority, said:

> As we expand our use of technologies, such as data-sharing and driverless vehicles, the threat keeps growing. Public transportation agencies of all sizes and at all locations are at risk. This is why I have made cybersecurity one of my top priorities.[11]

In 2019, a Leadership APTA Class focused on cybersecurity and as its capstone project produced, "*Ensuring Cyber Security for Public Transit Agencies in the Age of Autonomy*."[12] Also in 2019, APTA produced a training video for transit executives called "Cybersecurity Fundamentals for Executives."[13]

There are two vectors of change affecting transit agencies that exacerbate transit systems' cybersecurity exposure and will continue to add pressure for more oversight from both federal and state entities. The first vector of change is data. Transit agencies today are generating increasingly large volumes of data. For the average agency, however, these data remain siloed and sparsely integrated with other internal or—more importantly—external systems.

To date, this fragmented architecture has stunted malicious actors' efforts to access transit agencies' data. However, more systems, processes, and applications are coming online that will enable and require transit agencies to stitch together their data, both within their organization and in collaboration with other public and private organizations. In the same interview, Mr. Ford stated:

> The risks of operating in this cyber-environment are broad and deep, requiring elevated levels of awareness and response to potential attacks that can do lasting damage to hard assets, like infrastructure, and soft ones, like reputation. Increasingly, protecting these assets is a strategic priority and an operational imperative.[14]

Data at risk include employee information and operational data, as well as customer and financial data. As the connected nature of this data patchwork grows, so too will the frequency with which malicious actors target that data for theft or disruption.

Hackers Attack Transit System in California's Capital

In November 2017, Sacramento Regional Transit (SaRT) suffered a ransomware attack, crippling its website and destroying the underlying data.

What Happened: Hackers gained access to the transit agency's website and destroyed all data, taking the website offline. They then requested a ransom of one bitcoin (worth approximately $8,000 at the time). The agency did not pay the ransom.

The Response: SaRT was able to restore 80% of the website within days using backups. The full scope of the breach remained unclear, however, due to limited practices of logging data.[15]

In parallel, a second emerging vector of change is the increasingly connected nature of transit activities. The increased use of sophisticated technology in various aspects of the transit industry has exacerbated the potential for large-scale disruption to the nation's transit activities. Vehicle connectivity is expansive. Numerous technologies are already in the field, including global positioning systems (GPS), Wi-Fi, cellular, radio, and dedicated short range communications (DSRC). 5G and other emerging technologies are on the horizon. These technologies now allow transit agencies to send data back and forth between their vehicles and the command center, other vehicles, and the internet, in real time.

Tangential to the data patchwork described above, vehicle connectivity is not only making the data integrated and systemically accessible; it is also making accessible the data from the operation of the vehicle itself in digital form. The ability for a malicious actor, with the right access and capabilities, to alter the operation of vehicles—potentially at scale—will become technically feasible as more vehicles are digitally connected in some fashion, from buses to trucks to trains and even ferries.

Hackers Hijack a Big Rig Truck's Accelerator and Brakes

In 2016, researchers were able to successfully hack a 2006 semi-truck and a 2001 school bus and take control over the vehicles' operations.

What Happened: Researchers "managed to speed up the truck against the driver's will… and they found that, at least when the bus was in neutral with the parking brake on, their engine-revving hack worked on the school bus, too."

The Response: "It is imperative that the trucking industry begins to take software security more seriously," the Michigan researchers conclude in their paper describing their work.[16]

Add to these trends the already painful examples of ransomware and other active attacks occurring with alarming frequency. It is well past time for transit agencies to seriously invest in cybersecurity, from adequate resourcing and implementing best practices for threat mitigation to developing robust systems and plans to recover as incidents arise. Current guidance and support for transit agencies exists, but it requires that transit agencies invest and ensure agency-wide understanding and compliance. Regulations are sparse, but, in many cases, best practices do exist, and change is underway. Transit agencies that move forward now will not only be safer from disruption from cybersecurity threats: they will also be better positioned to meet and influence federal, state, and other regulatory actions undoubtedly on the horizon.

REPORT ORGANIZATION

Section I of the report provides an introduction to the transit industry and the growing risks that cybersecurity presents. Section II provides a summary of the methods used to research the subject matter and compile this report. In Section III, the authors discuss transit operations' cyber vulnerabilities and risks. Section IV provides a review of the guidance available to transit agencies. Section V explores the findings from this study. Section VI provides policy recommendations to better support cybersecurity readiness among public transit agencies.

II. METHODOLOGY

This study employed a multi-method approach to research and evaluate the status of public transit agencies' cyber preparedness and to develop policy recommendations to enhance those levels of preparedness. The study focused on public surface transit agencies that receive funding from the FTA and operate in the United States. Private agencies and agencies that serve other countries were considered out of the study's scope. Only agencies that provide surface transit were considered; all other modes were excluded.

1. **Literature Review.** The authors reviewed literature on physical and digital cybersecurity strategies in transit as well as other industries and applied key findings from this review to develop oral and digital surveys and policy recommendations. The authors supplemented the literature review with an internet search of recent cyber incidents and innovative and emerging trends in cybersecurity. Many of the online resources filled gaps in the literature where existing publications had not kept pace with cybersecurity practices and innovations. Finally, the authors attended relevant sessions at the 2019 APTATech Technology Conference, the 2019 APTA Annual Conference, the 2019 ITS World Congress, and the 2020 Transportation Research Board Meeting.

2. **Expert Interviews.** Between winter 2019 and spring 2020, the authors developed an interview protocol and conducted three groupings of expert interviews. In the interview process, the authors were careful to walk through all of the scripted questions with each interview subject, but the discussion was otherwise unstructured, which enabled the authors to explore specific experiences and anecdotes that the interview subjects were able to contribute on the topics at hand. The first group, interviews with transit operators, was led by Scott Belcher and Brandon Thomas, and it entailed anonymous interviews with 26 transit chief executives or chief security officers (whose titles differed by organization and ranged from Chief Information Security Officer to Chief Technology Officer to IT professional). These interviews gathered data from 20 public transit operations and were representative of the size, geographic scope, and diverse nature of the nation's public transit operators. The second group, interviews with transit professionals not currently employed by transit operators, was led by Scott Belcher, Brandon Thomas, Eric Greenwald, and Ed Merlis.[17] The third group, interviews with government officials, was led by Eric Greenwald, Scott Belcher, and Ed Merlis. These interviews included representatives of the U.S. DOT, the FTA, the U.S. Department of Homeland Security (DHS, in particular the DHS' Cybersecurity Infrastructure and Security Agency, CISA), the Transportation Security Administration (TSA), the White House Office of Science and Technology Policy (OSTP), and professional staff from both the United States House of Representatives and the United States Senate. Twenty-two professionals were interviewed, a number of interviews that the authors requested with Hill staff could not be completed given the nature of the study and availability of key staffers during the uncharacteristically busy period in which the interviews were conducted. Copies of the interview questions are attached as appendices.

3. **Digital Survey.** Based on the information gathered in the literature review and the oral interviews, the authors developed a digital survey that was sent to U.S.-based public transit operator executives during the winter of 2020. Survey responses were matched with data from the NTD. APTA provided the authors a list of 327 executives (APTA members who lead public transit agencies registered in the NTD), of which 312 were unique. Of these 312 executives, 287 were U.S.-based operators.[18] APTA members represent the vast majority of the U.S. industry in terms of populations served, unlinked passenger trips, and passenger miles. APTA reports that more than 90% of the American and Canadian population using public transportation use services provided by APTA members.[19]

   From the 312 surveys issued, the authors received 104 total responses and culled those to 90 by eliminating incomplete responses, responses that could not be definitively correlated with a specific transit agency in the NTD, duplicate responses, and responses from non-U.S. operators, yielding an overall survey response rate of 31%.

   Altogether, the agencies that responded to the survey serve over 124 million people—roughly a third of the entire population of the United States. Of the 90 agencies, only five (6% of respondents) are considered rural, having lower populations than the general population and being less subject to emerging trends in mobility.[20] Rural agencies are subject to fewer FTA reporting requirements. Nearly 60% of public transit agencies in the NTD are rural, but they comprise just over one percent of the transit trips in the United States.[21] The authors recognize that rural agencies are underrepresented in the survey data collected; the 85 other agencies that responded to the survey serve populations of 50,000 or more.

   A more detailed review of the populations that survey respondents serve shows a fairly broad distribution (Figure 4).

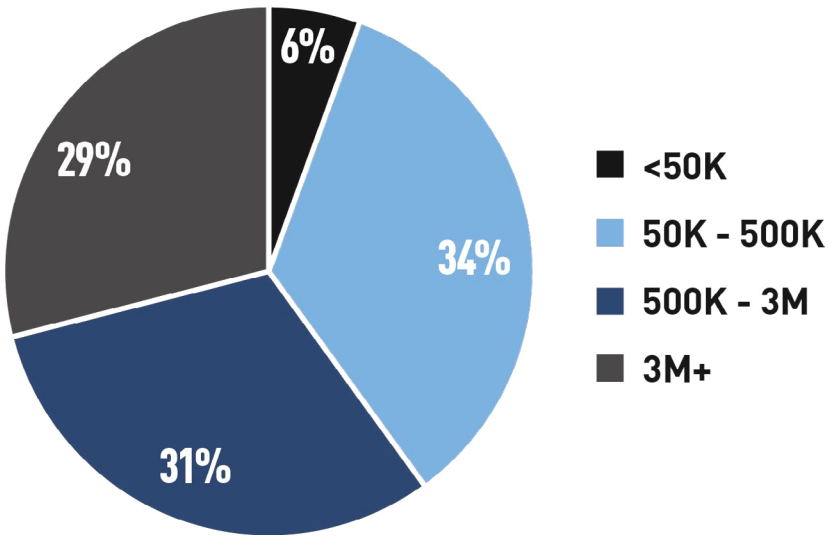


Figure 4. Population Served by Survey Respondents[22]

The survey netted a similarly broad distribution with respect to the organizational size of the responding entities. Agencies ranged in size from $100K to $1B+ in operating expenses (Figure 5). Of the agencies surveyed, 17% were small (<$10M in operating expenses) and 33% were extra-large (>$100M in operating expenses).[23] Where the data identifies differences between the size of the agency that appear to be based solely on size or on the rural nature of the of transit agency, these differences are called out for the reader.

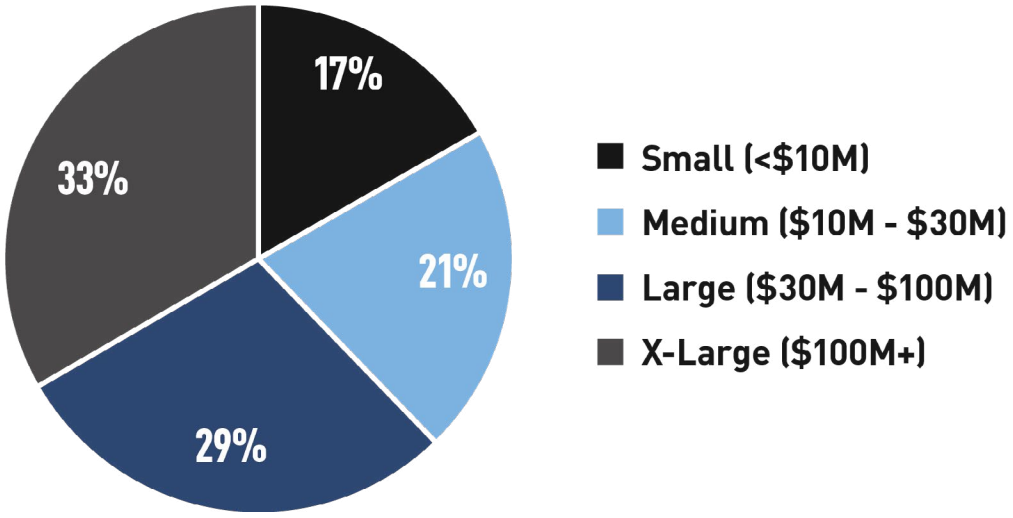


Figure 5. Agency Size of Survey Respondents[24]

4. **Policy Recommendations.** The authors identified three focus areas for recommendations: the Executive Branch, the Legislature, and Industry/Association.

5. **Limitations of Study.** The intent of this study is to assess the readiness, resources, and structure of public transit agencies to identify, protect from, detect, respond to, and recover from cybersecurity vulnerabilities and threats.[25] The authors excluded private entities involved in transit (e.g., auto manufacturers; private bus and rail companies; mobility on demand (MOD) companies that include car, bike, scooter, and share companies).

   Further, while the authors conducted an assessment of the threats currently facing the transit industry, they did not closely examine emerging technologies that will soon be widely used in transit, such as connected vehicles (i.e., vehicles that communicate with each other to prevent crashes) or autonomous vehicles. In this report, the authors focused on identifying general measures to improve cybersecurity for transit agencies in a manner that is agnostic to the specific technologies that those agencies employ.

   The authors did not assess the internal cybersecurity capabilities of public or private organizations with whom many agencies integrate and/or share data, such as major industry vendors, trade associations, and/or federal agencies such as U.S. DOT or DHS.

Finally, this report was written as the COVID-19 pandemic spread across the globe. The authors made no attempt to predict what the transit industry would look like after COVID-19; however, the principles set forth in this report will be as relevant, if not more relevant, in a post-pandemic environment.

III. TRANSIT CYBERSECURITY RISK PROFILE

Like every facet of society, public transit has been going through multiple waves of technological evolution. Every aspect of transit operations is subject to change, whether it is routing, scheduling, or payment. Payment has moved from fare boxes, in which riders inserted cash or coins, to payment by smartphone and digital wallet. Routing changes that were once done manually were so time- and labor-intensive that they rarely occurred; now, they can be done with modern mapping technology, artificial intelligence, and machine learning, as well as better software. Transit operators can now run real-time route scenarios to optimize their services. Knowing when and where to catch the next bus used to require a series of paper printouts and signs. Today, riders can not only obtain this information on their smartphones, but it will also be updated in real time.

The modern transit operator collects and maintains an ever-increasing volume of data concerning its operating systems, vehicles, employees, and customers. Buses transmit operator communications, bus operations data, and in some cases, live video and rider internet activity. This data "exhaust," as many in the technology world refer to it, has made public transit more convenient, safer, and more efficient. Automatic passenger counters, centrally aided dispatch, automatic vehicle location software, and real-time bus arrival systems have improved transit operations. Similarly, technologies such as traffic signal preemption, dynamic rerouting, and lane departure warning systems have also increased buses' and transit systems' safety and efficiency (Figure 6).

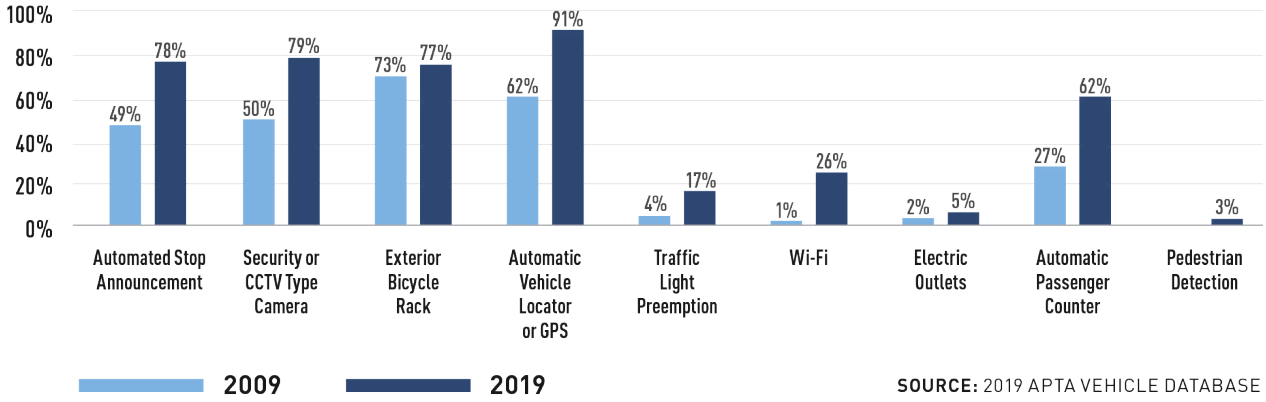


Figure 6. Percentage of Buses with Passenger Equipment, 2009–2019[26]

Transit systems have also become increasingly complex, owing to an ever-increasing use of transportation network companies (TNCs), first- and last-mile MOD services, and mobility-as-a-service (MaaS) options. Public transportation agencies are becoming "mobility hubs," where riders are able to manage their use of public transit as well as MOD services that are often provided by private companies such as shared-use cars, scooters, bikes, or skateboards, taxis, or autonomous shuttles.

This changing transportation environment is forcing transit agencies to rethink their business strategies as well as their offerings. Are they bus or subway companies, or mobility providers? If they are mobility providers, how do they compete with massive Silicon Valley

companies like Alphabet or Uber, or with nimble start-ups like Via or Moovit?

COVID-19 has only exacerbated the need for transit agencies to adapt and change. To succeed, however, these agencies need not "do it all." There is no shame in outsourcing aspects of their offerings, if that is the most efficient means to deliver services. Transit agencies need to focus on what they do well, contract out what they don't, and leverage technology and data, lest they be left behind. Meeting rider demand requires adopting new technologies and services that transit operators are only beginning to understand, much less fully integrate into their security operations.

TRENDS IN TRANSIT

Public transit agencies are contracting out aspects of their system with increasing regularity. Most agencies have historically contracted with a limited number of companies that dominated the market with proprietary hardware and software. One Chief Innovation Officer shared that her organization, like many others, had "two key vendors that provide the majority of our software and hardware, but as we modernize, we are looking to implement a more modular infrastructure."[27]

This is the way it has been, but it is not the way it will remain. In a world of on-demand travel, TNCs, artificial intelligence, multimodal trip planners, and so on, incumbent vendors are under direct threat from start-ups and new entrants adept at integrating with application program interfaces (APIs). The age of the one-stop shop for an agency's technology needs is waning. Many incumbent vendors will not survive, but neither will the average public transit agency if it does not get smart about the changing nature of the market and, by extension, the increasing risks of cybersecurity vulnerabilities.

Each time a new technology, a new connection, a new data source, or a new vendor is added to a transit agency's network, so too is a new range of cybersecurity vulnerabilities. Ironically, the public transit agencies that have been slowest to modernize their fleets and their operations are the least likely to become cybersecurity targets, as they have fewer access points. However, they are also the ones least likely to survive this technological revolution, as they are less equipped to understand and adapt to shifts in ridership behavior and the changing needs of their community.

Companies like Uber and Lyft have cherry-picked riders with lesser or no subsidies away from traditional fixed-route services, creating direct competition with public transit agencies for ridership. To address this new competition, many public transit agencies have partnered with these same companies to provide new or expanded service offerings: an alliance of enemies of sorts. MOD has become a battleground for public transit agencies. Historically, transit agencies have provided limited first-/last-mile services, paratransit supplements, or micro-transit services. APTA's *2019 Fare Database* recorded 36 transit agencies with mobility pilots, either with Uber, Lyft, other private operators, or in-house operators.[28] Some agencies are now evolving into mobility hubs for an entire region.

Many private companies such as Genfare, Bytemark, and Transit serve as vendors for MOD services to transit agencies, while some public transit agencies offer their own

version (e.g., DART). Each has its own platform for data management, privacy, and risk. As transit agencies have struggled with this new paradigm, so too have private vendors. Some have failed, such as Chariot and Moovel, while others have consolidated or have been purchased: Intel bought Moovit, Trapeze entered into a strategic partnership with Masabi, Uber transferred its electric bike/scooter company Jump to Lime and led a $170M investment round in Lime, while both were taking significant losses and laying off staff.[29] The key take-away from this changing mobility landscape is that it will continue to be unstable and that the transit experience will be based on new forms of connectivity, which leads to new forms of vulnerability.

RISK IN TRANSIT

As noted above, failing to modernize could result in the public transit agency becoming irrelevant, but modernizing carries with it the risk of exposing riders and the general public to a different, growing array of threats. Those transit agencies that have learned to adopt new technologies to improve efficiency in operations have not necessarily adopted technology to minimize vulnerability to cybersecurity threats at the same rate.[30]

While the survey results do not provide detailed information on the adoption of effective cybersecurity measures, some of the data do reveal a prevalent underappreciation of the scale and nature of the threat. Most of the agencies that responded to the survey claimed they had not yet had many (or any) cybersecurity incidents. Of the 90 agencies that responded to the survey, only 20 (22%) admitted to having experienced a cybersecurity incident where more than 1,000 records were breached, over $10K in losses were incurred, or an operating system was down for more than one hour (Figure 7).[31] This reporting seems highly suspect, as will be discussed in the findings section.

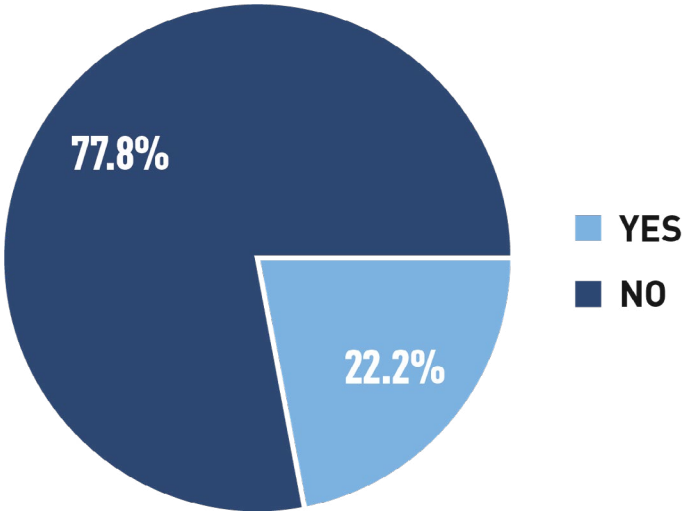


Figure 7. Have You Had an Incident?

By comparison, Dell Technologies surveyed over 1,000 IT professionals from public and private organizations with over 250 employees across various industries and found that 82% had suffered a disruptive event (defined as downtime or data loss). Though this comparison is not direct, given the ambiguity in the thresholds assumed in the Dell survey, Section V discusses in more detail reasons to suggest most public transit agencies are unaware of cyber intrusion activity that may be happening among their systems.

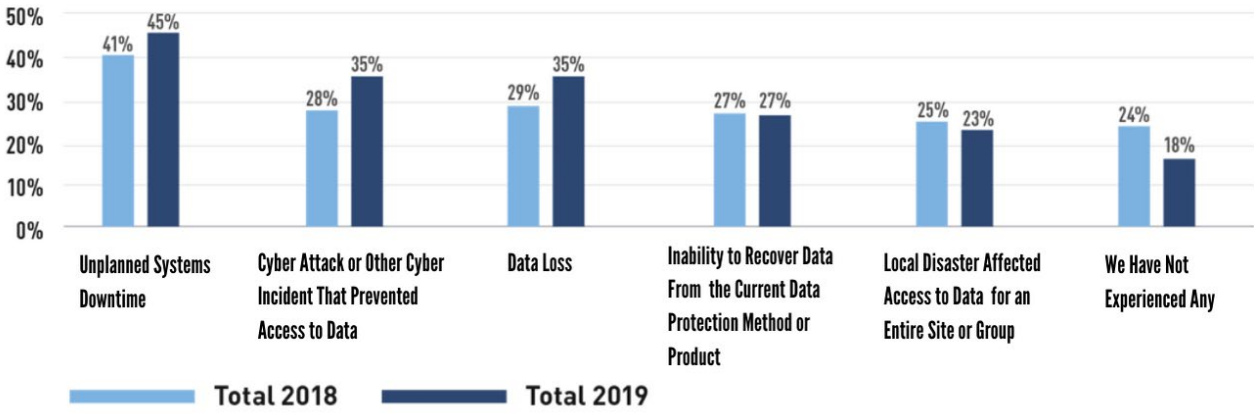


Figure 8. Percentage of Global Organizations That Suffered From a Disruptive Event[32]

Threat Vectors

In general, the transportation sector faces the same spectrum of cyber threats as most industries that rely heavily on technology. What distinguishes transit agencies from other potential targets of cyber-attack is the nature and severity of potential consequences that could result from cyber-attacks to transit operators. These range from routine website outages and theft (similar to what that many companies face) to nightmare scenarios involving substantial loss of life and massive property damage that could result from malicious actors remotely targeting transit systems.

Phishing and Business Email Compromise

Phishing is the fraudulent attempt to obtain sensitive information such as usernames, passwords, and credit card details by disguising oneself as a trustworthy entity in an electronic communication. In the most common vector for phishing attacks, the malicious actor induces the recipient to click on a link that sends the recipient to a website that either directly drops malicious code on the recipient's computer or tricks the recipient into revealing account credentials (username and password), enabling the attacker to then impersonate the recipient and gain access to that account.

In a 2018 study, F5 Labs found that "phishing continues to be a top attack vector and, in many cases, is the tried-and-true, go-to attack vector in multi-vector attacks."[33] Phishing is particularly important because it provides the attacker access to important accounts and can be the entry point to other types of cyber-attacks. Transit operators can be attractive phishing targets because of their large and often dispersed workforce—and the potential for a lucrative return given the value of such data. One of the 2019 Leadership APTA Class capstone projects focused on cybersecurity and found that phishing is by far the most common type of cyber-attack.[34]

Business Email Compromise (BEC) is a more targeted and sophisticated form of phishing, in which the malicious actor impersonates a CEO or other high-level official within a company, usually with the intent of tricking the recipient into transferring money to a bank account controlled by the malicious actor. In 2018, the FBI reported that thieves used BEC scams to collect more than $12 billion between 2013 and 2018.[35]

With respect to BEC attacks, transit agencies face the same sort of risks from these threat vectors as most companies; however, while these attacks are typically used by criminals simply seeking financial gain, their low risk, low cost, and generally high probability of success means that they also serve as the initial point of entry for malicious actors seeking to do even more damage.

Data Breaches

Data breaches have become a bigger part of the general consciousness as more and larger breaches by more prominent organizations have been discovered in recent years. The type of breach most often to hit the news is one that affects customers, because it results in the loss of the customers' personally identifiable information (PII). Typically, the primary impact on companies suffering a data breach is the cost associated with (1) technical remediation of the breach, (2) notification to the victims, and (3) provision of defense against the numerous lawsuits (e.g., from customers, shareholders, and state attorneys general). In a 2019 report, IBM and the Ponemon Institute released a report finding that data breaches increased by 130% from 2006 to 2019. The report estimated the average cost of a breach in the United States at $8.19 million.[36]

It's worth highlighting that victim notification requirements are driven by state law, which can vary significantly from one jurisdiction to the next.[37] This effectively amounts to an additional (and complex) set of compliance requirements completely separate from the transit-sector specific regulations that arise at the federal level. Not only is compliance with this patchwork set of laws proving to be increasingly costly, but failure to do so carries an increasing risk of investigation from state prosecutors.

There have been a number of recent high-profile incidents causing regulators to take a more active role in investigating data breaches. There have been increases in the number of inquiries, the speed with which they are made and the number of jurisdictions in which they are brought. [38]

While malicious actors targeting customer data can monetize that data in a variety of ways, the most plentiful source is typically customer payment information. For many transit agencies, customer payment information is rather limited because most agencies outsource their payment processing. Most payment transactions are governed by Payment Card Industry Data Security Standard (PCI DSS), a set of compliance requirements established by the PCI Security Standards Council. This industry standard was designed to reduce the risk and cost of credit card fraud. It is precisely because this standard imposes fairly stringent security requirements that the vast majority of transit agencies have outsourced their payment processing.

PCI Security

The PCI Security Standards Council touches the lives of hundreds of millions of people worldwide. A global organization, it maintains, evolves, and promotes Payment Card Industry standards for the safety of cardholder data across the globe.

The Council serves those who work with and are associated with payment cards. This includes: merchants of all sizes, financial institutions, point-of-sale vendors, and hardware and software developers who create and operate the global infrastructure for processing payments.

The Council has two priorities:

1. Helping merchants and financial institutions understand and implement standards for security policies, technologies, and ongoing processes that protect their payment systems from breaches and theft of cardholder data.
2. Helping vendors understand and implement standards for creating secure payment solutions.[39]

Figure 9 shows that among public transit agencies surveyed, 84% do not manage customer payment information. This places the onus of data security less on the agency and more on the vendor, and those vendors are generally subject to strict security standards under PCI DSS.

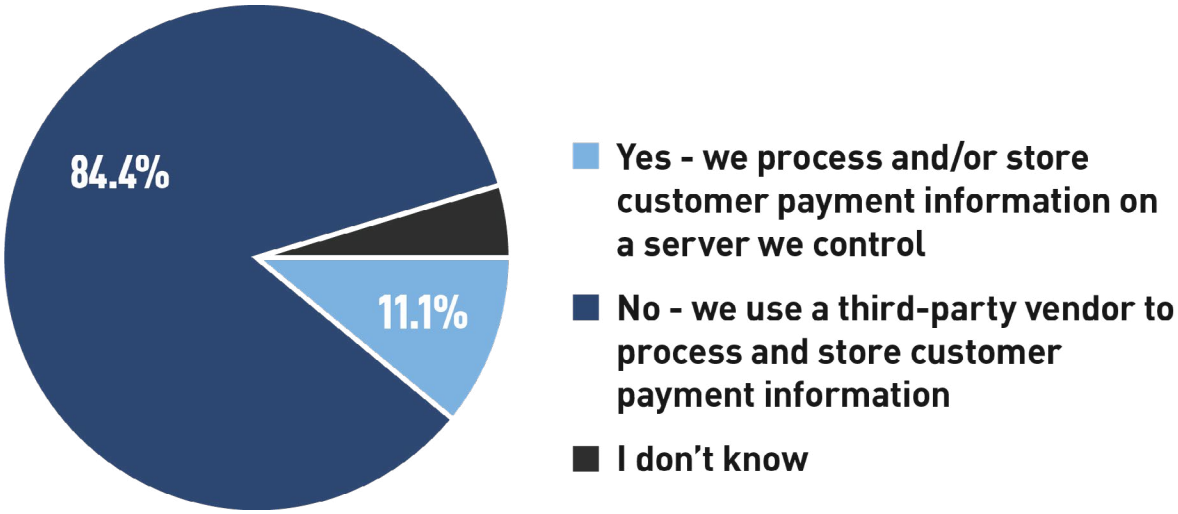


Figure 9. Do You Process and/or Store Customer Payment Information Directly?

Although most transit agencies outsource their payment activities, all transit agencies have little choice but to retain sensitive data on their own employees. Employee data often include social security numbers, dates of birth, and other critical identifying information. This type of data, while usually found in smaller volumes than troves of payment data, is often more valuable to criminals, as there is a robust market for the kind of sensitive information found

in employee records. At many agencies, the tools used to manage this data are rudimentary. Sharing is conducted using spreadsheets, email, and other unsecure channels.

Compromise of Operational Networks

While transit agencies are justified in focusing on loss of customer and employee data, the compromise of operational data, such as running industrial control systems, traffic signals, and emergency communications networks, brings with it the potential for far more destructive consequences. Experts believe that there is not enough focus on operational technology and business interruption concerns.[40]

Among public transit agencies, there is a growing understanding of the value of operational data, particularly as data are leveraged to improve service. However, driving advances in efficiency without corresponding improvements in security will leave agencies exposed and at risk. Adam Cottini, managing director of the cyber liability practice with Gallagher, a global leader in insurance and risk management, stated that "the critical processes themselves could be vulnerable to attacks which could lead to business interruption, cyber ransomware, and potentially data protection."[41] Beyond a serious interruption in operations, transit agencies may be targeted for destructive and potentially deadly cyber-attacks.

> Unlike many industries, where the potential consequences of poor cybersecurity are largely financial or privacy-driven, an attack on a public transit system has the potential to be lethal. Vulnerable supervisory control and data acquisition (SCADA) systems could be hijacked by terrorists or cyber-criminals to cause derailments or collisions. While this nightmare scenario has not yet occurred, there have been numerous incidents involving mass transit and other SCADA-dependent industries that paint a clear picture of how it could happen.[42]

Good operational security would dictate isolating these networks from the internet and only allowing access from within a transit agency's physical facilities. However, poor understanding of security practices and the compelling desire for efficiency that comes with remote access and operation frequently overrides what should be an imperative to protect these critical systems.

Ransomware

Ransomware attacks, particularly among city agencies, have increased in recent years. In such situations, the attacker seeks to take control of the organization's systems or data. Control can be taken in the form of resetting administrator passwords or encrypting key databases. The attacker then asks for payment to return control back to the organization.

Ransomware is software that infects computer systems. Attackers infiltrate the system often through a single device and the program spreads from one device to another. As the infection promulgates, data is corrupted beyond use. Often as part of the spread, the attacker provides an "extortion message" declaring its demands for restoring the system.

> The demand often includes a series of deadlines for payment: each missed deadline leads to a higher ransom demand and perhaps some destroyed files. If the victim

fails to pay, the attacker discards the decryption keys, making the data permanently inaccessible.[43]

For transit agencies, ransomware presents an outsized risk. If malicious actors are able to lock up critical data, the suspension of all operational activity could result. The strategy promoted by law enforcement has long been to discourage paying ransom demands. As a result, organizations are left to restore access on their own or to rely on data archives or other resources to restore systems. This is feasible for some, but certainly not for all transit agencies—especially those agencies that have not planned for such a scenario.

Table 1. Ransomware Growth in the U.S.[44]

According to the FBI's Internet Crime Complaint Center, the number of victims reporting ransomware attacks has declined in recent years, though there was an increase in 2019. However, the amount demanded—and paid—is on the rise, with the average ransom in 2019 growing more than sixfold from 2015. Attackers are more selective and tend to go after larger companies that will likely pay but do not have the IT staff to handle a recovery. The losses do not include business losses (such as wages, files, third-party remediation). The FBI said not all victims reported the actual loss, so the amounts could be low.

Date	Victims	Victim Losses	Average Loss per Victim
2019	2,047	$8,965,847	$4,380
2018	1,493	$3,621,857	$2,426
2017	1,783	$2,344,365	$1,315
2016	2,673	$2,431,261	$910
2015	2,453	$1,620,814	$661

Source: The Colorado Sun

Debbi Blyth, the Chief Information Security Officer for the State of Colorado, relayed the story of how the Colorado Department of Transportation's (CDOT) network was taken down, brought back, and then taken down again by malware known as SamSam: "the impact was fast and furious… server administrators, database administrators, backup administrators and hundreds of calls to the help desk—and that was all in the hour or first couple hours of opening for business."[45]

In at least one sense, CDOT was fortunate, as the attack only impacted their business networks with a total recovery cost of $1.7 million. The authors do not have data with which to estimate the probable cost to a transit agency of operations disrupted by ransomware, but the transportation logistics industry does. Shipping giant Maersk suffered approximately $200 million in losses as a result of the NotPetya ransomware,[46] and the Australian company TollGroup is still tallying up the costs from its second ransomware attack in three months.

Vendor Management

Effective cybersecurity management does not end at the edge of an organization's systems: successful strategies and plans must also include vendors that support operations. Any weakness in a vendor is a weakness for all the organizations it supports.

Vendors are a common attack vector for malicious actors, as those companies often have trusted relationships with their customers. The exploitation of this trust relationship can be as simple as luring an employee to click on a link in an email that appears to be coming from the vendor, or it can be as complex as compromising a direct connection between the vendor's network and that of the transit agency.[47]

Target Hacked

In the 2013 retail giant Target was compromised by hackers that stole credentials from a third-party vendor that provided refrigeration, heating, and air conditioning services to Target. The vendor was provided direct access to the Target computer networks (possibly for the purpose of monitoring energy consumption at Target facilities). The attackers were able to compromise Target's payment system network through the third-party vendor's network access.

Effective cybersecurity management among vendors begins with contracts. Standard clauses are included in contracts that center on cybersecurity audit requirements, monitoring requirements, and notification requirements. Audit requirements typically ensure a third party is engaged periodically to confirm compliance. For some, certain requirements are made clarifying who can provide such audit services, such as firms with U.S. ownership or certain accreditations. Most stipulate how often an external audit must be conducted, as well as the documentation that must be shared with the client. Monitoring requirements can include specifications regarding what data are tracked and how long they are stored. Notification requirements define what situations warrant notification to the customer or client, and in what time frame.

For reference, 41% of public transit agencies surveyed said they do not currently have standard clauses related to cybersecurity currently included in their vendor contracts. An additional 21% responded that they did not know whether they included such clauses in their vendor contracts (see Figure 10). These numbers are inherently troubling, but they also raise questions as to the sophistication of the standard clauses that transit agencies have inserted in their vendor contracts—and the extent to which the requirements in those clauses are monitored, enforced, or even understood by those who include the clauses in the contract.

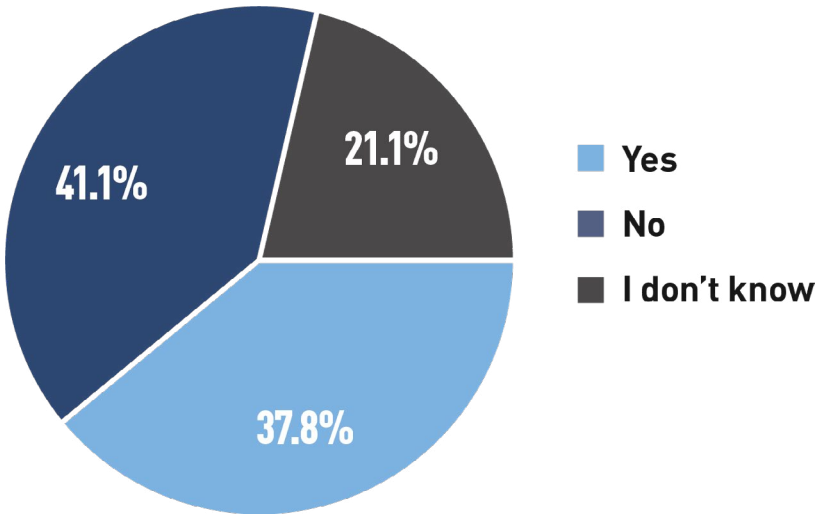


Figure 10. Do You Have Standard Clauses in Your Vendor Contracts Related to Cybersecurity?

These clauses are designed to require that vendors implement basic cybersecurity measures to reduce the likelihood that malicious actors are able to exploit the vendor's systems and then leverage that exploit to attack the transit agency.

Beyond contract clauses establishing cybersecurity requirements, vendor management related to cybersecurity can be very valuable for ensuring the necessary measures are in place to reduce exposure and mitigate impacts as incidents occur. Physically reviewing operations and asking questions about access and system credentials can help convey to the vendor the seriousness of cybersecurity. Cybersecurity requirements established through vendor contracts can provide a solid basis on which to manage vendors' cybersecurity practices. This can be an especially valuable tool for those operators that have resource constraints.

Counterfeit Hardware

It is easy to assume that the BART counterfeit hardware example provided in the introduction to this report is an anomaly or a one-off. Unfortunately, it is anything but. That incident alone led to the discovery of counterfeit hardware in a number of U.S. transit operations, all from the same contractor. In 2012, the Senate Committee on Armed Services issued a sobering report on the volume of counterfeit electronics being sold to the various departments of the armed services and the major U.S. companies that serve them such as BAE, Boeing, Lockheed, and Honeywell.[48]

> The Committee's investigation uncovered overwhelming evidence of large numbers of counterfeit parts making their way into critical defense systems. It revealed failures by defense contractors and the U.S. Department of Defense (DOD) to report counterfeit parts, as well as gaps in DOD's knowledge of the scope and impact of such parts on defense systems.[49]

Despite the serious conclusions from this eight-year-old Senate report, malicious actors continue to use hardware as a means of accessing cyber networks. In 2017, DHS seized more than 34,000 shipments of counterfeit and pirated products. Approximately 12% of the shipments seized were health-, safety-, and security-related products.[50] With budget constraints and limited tools accessible, transit agencies remain vulnerable on this front.

Supply Chain Risk Management

On May 15, 2019, the White House issued Executive Order (EO) 13873, *Securing the Information and Communications Technology and Services Supply Chain*, which will have cascading effects for transportation as well as other sectors.[51] The EO covers broad-based Information and Communications Technology (ICT) and supply chain risk, encompassing 5G network gear, and it is much more than a ban on Huawei.

Huawei is a Chinese multinational information technology and consumer electronics company that has been accused by the United States and other nations of corporate espionage and intellectual property theft. In 2019, Huawei was restricted from engaging in commerce with U.S. companies resulting from allegations that it willfully exported technology of U.S. origin to Iran in violation of U.S. sanctions. The May 15, 2019 EO bans any entity that is "owned by, controlled by, or subject to the jurisdiction or direction of a foreign adversary" from doing business in the U.S. and will impact every mode of transportation, including aviation, transit, rail, maritime, trucking, autonomous vehicles, and drones, among others.

In December 2019, Donald Trump signed into law the National Defense Authorization Act for 2020, which included a provision banning the use of federal funds to purchase "rolling stock" (e.g., cars, vans, buses, rail cars) made by companies "owned or controlled" by countries that the U.S. Trade Representative has identified on its Priority Watch List.[52] The ban is to take effect on December 20, 2021. While the Executive Branch is still in the process of finalizing this list, the most relevant country to be subject to these restrictions is China whose electric bus manufacturer BYD has manufactured over 400 buses in Lancaster, PA, and has the most electric buses in operation in the United States.

These efforts reflect a growing concern over cyber supply chain risk management in the transit sector. Other sectors have been gradually waking up to the realization that the technological equipment they purchase may suffer from pervasive vulnerabilities before it is even connected to their business or operational networks. Whether due to insufficient security in the engineering of the hardware, software, or firmware; compromise of the industrial process by nation-state actors; or active collaboration between the manufacturer and these actors, the reality is that, owing to the highly distributed, global manufacturing process, virtually no supply chain can be guaranteed secure.

As with other areas of risk, public transit agencies have been slow to respond to this threat. Of the transit agencies that participated in the oral interviews Washington, D.C.'s Metropolitan Area Transit Authority (WMATA) described their active and robust supply chain risk management program. Such a sophisticated program is beyond the resources of all but the largest transit agencies, but each transit agency is exposed to the risk.

WMATA's Supply Chain Cybersecurity Program

WMATA began putting in place a robust Supply Chain Cybersecurity Program over the past year. While still in its developmental phases, it has matured substantially over the last six months. Its progress has been expedited by Congressional interest in Chinese manufacturing.

WMATA's approach is to start with the premise that all procured information and operation technology is inherently at risk, regardless of where it is manufactured. The WMATA program starts by including a cybersecurity professional as an approver in all procurements involving technology. This can be a challenge, as technology is often baked into complex solicitations, like building a new rail station, which can slip through the cracks if the project manager or contracting officer does not realize what "technology" is exactly. Closed circuit television (CCTV) cameras, elevators or escalators, and information displays are examples of elements of a procurement that are tied to information technology but can easily be overlooked.

Once the cybersecurity team gets a procurement, they then look to apply standard language around things like protecting data (e.g., encryption standards), locking down open ports or permissions (e.g., access control), not using default passwords, and so on. WMATA has built a guide of standard language that the supply chain team can cut and paste from, ensuring a consistent application of standards. This standardization helps measure cost implications across procurements and helps steer vendors towards reasonable solutions, as often WMATA's requirements are the first they have encountered and can seem unreasonable at first blush. This process requires risk analysis and customization. The requirements exist on a scale of stringency based on the types of systems involved or data processed (e.g., does the new technology support train control versus elevator control, does the system process PCI data).

Of course, a portion of the team's time in this first year has been spent on educating WMATA's own workforce. For many employees who have been buying this standard technology for years (or decades) without cybersecurity involvement, the added time and cost can be unexpected. Once the language is accepted by the organization, the team will need to dedicate time to evaluating vendor responses to these new issues. This phase cannot be overlooked and can be very time-consuming. However, WMATA has concluded that if they don't measure the effectiveness of the solutions offered, there is very little point in instituting the requirements in the first place.[53]

IV. EXISTING CYBERSECURITY GUIDANCE FOR TRANSIT

The existing cybersecurity guidance for public transit is spread across numerous government and industry entities. This section gives a broad overview of the guidance available to the transit industry and highlights the major documents provided by both the regulatory bodies as well as non-profit trade associations. This overview is meant to direct researchers and individual transit agencies towards the most meaningful documents that can guide them in developing their own cybersecurity plans.

Given this complexity, there is limited accountability for cybersecurity programs among public transit agencies. Despite this limited accountability, federal resources exist for agencies to improve their cybersecurity readiness. Executive Order 13800, *Strengthening the Cybersecurity of Federal Networks and Critical Infrastructure*, makes federal agencies accountable for managing cybersecurity risks to their ecosystem, and it further encourages them to work with all entities to adopt the National Institute of Standards and Technology (NIST) Cybersecurity Framework.[54] Federal agencies directly involved in supporting Transportation System Sector (TSS) cybersecurity preparedness include NIST, DHS, and the U.S. DOT.

With the rise of the internet, digital, and connected systems, DHS, among other agencies, has developed an array of both offensive and defensive tools and tactics to protect against cyber threats. The bulk of this work is focused on what is deemed to be critical infrastructure.

> There are 16 critical infrastructure sectors whose assets, systems, and networks, whether physical or virtual, are considered so vital to the United States that their incapacitation or destruction would have a debilitating effect on security, national economic security, or national public health or safety.[55]

The TSS is the sector on that list in which public transit agencies sit. Given this label, DHS and other federal agencies are not only accountable, but they are also mandated to support the security of America's transit systems, both their physical and digital components. Moreover, as noted above, the risk profile of these systems is increasing as technology evolves. However, to date, the regulatory regime is behind in establishing the necessary regulation, compliance requirements, and oversight to ensure the nation's transit systems adequately address current and future cybersecurity threats. The existing regulatory and oversight gap is increasing as the role of technology expands in the functioning and efficiency of how transit systems operate.

On February 12, 2013, the White House released Presidential Policy Directive 21 outlining the federal government's responsibility to strengthen the security and resilience of U.S. critical infrastructure against both physical and cyber threats.[56] The Directive established that DHS and U.S. DOT share responsibility for the TSS. In sharing this role, the DHS's and U.S. DOT's responsibilities include:

- Collaborating with critical infrastructure owners and operators
- Coordinating with state, local, tribal, and territorial entities to implement the directive

- Providing, supporting, or facilitating technical assistance and consultations to identify vulnerabilities and help mitigate incidents in the sector

THE NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY (NIST)

The foundation for much of the United States' cybersecurity efforts, including DHS and U.S. DOT, is the NIST Cybersecurity Framework. NIST is a non-regulatory agency: it has no authority to dictate the use of any particular standard. However, when there is a matter of public good that depends on establishing a standard, NIST convenes relevant public and private stakeholders to develop the standard, as they have done in the face of cybersecurity threats.

In February 2014, NIST released the Framework for Improving Critical Infrastructure Security in response to Presidential Executive Order 13636, *Improving Critical Infrastructure Cybersecurity*,[57] which called for a standardized security framework for critical infrastructure in the United States. It is not a how-to guide for cybersecurity; rather, it is a framework designed to help a wide range of organizations assess risk and make sound decisions about prioritizing and allocating resources to reduce the risk of compromise or failure in their computer networks. For any organization to leverage the NIST Framework, customized implementation is required in ways that are not necessarily obvious from the document.

NIST Cybersecurity Framework: Key Functions

Identify: develop the organizational understanding to manage cybersecurity risk to systems, assets, data, and capabilities;

Protect: develop and implement the appropriate safeguards to ensure delivery of critical infrastructure services;

Detect: develop and implement the appropriate activities to identify the occurrence of a cybersecurity event;

Respond: develop and implement the appropriate activities to take action regarding a detected cybersecurity event;

Recover: develop and implement the appropriate activities to maintain plans for resilience and to restore any capabilities or services that were impaired due to a cybersecurity event.[58]

U.S. DEPARTMENT OF HOMELAND SECURITY

Within DHS, there are two key entities responsible for addressing the cybersecurity needs of the TSS: the Cybersecurity and Infrastructure Agency (CISA) and the Transportation Security Agency (TSA).

Cybersecurity and Infrastructure Security Agency. CISA was formed in November 2018 with the purpose of building national capacity to defend against cyber-attacks. In

addition to its mission to improve protections for federal government computer systems, CISA also develops "trusted partnerships across the public and private sectors" to deliver "technical assistance and assessments."[59]

Transportation Security Administration. TSA's origins date back to the days after September 11, 2001, when it was formed as part of the Aviation and Transportation Security Act. Its "mission is to protect the nation's transportation systems to ensure freedom of movement for people and commerce."[60] Given its provenance, TSA's original orientation centered on physical security, but the agency "is responsible for securing the nation's transportation systems from all threats, including both physical and cyber."[61]

In this latter role, TSA overlaps with CISA. TSA explains the division of labor as follows:

> Although TSA has responsibility for oversight of both the physical security and cybersecurity of the [TSS], TSA is not directly responsible for the defense of the private sector portion of TSS information technology infrastructure. Rather, TSA serves a vital role in ensuring the cybersecurity resilience of the TSS infrastructure and will work with the Cybersecurity and Infrastructure Security Agency (CISA), with its mission to protect the critical infrastructure of the United States.[62]

In 2015, DHS built upon the NIST Framework and issued a document "to provide the TSS guidance, resource direction, and a directory of options to assist a TSS organization, [including public transit agencies], in adopting an industry-compatible version of the NIST Framework."[63] This guidance was designed both for transit agencies that have an existing risk-management program and for agencies that do not yet have a formal cybersecurity program.[64]

TSS Cybersecurity Framework Implementation Guidance

The TSS Cybersecurity Framework Implementation Guidance and its companion workbook provide an approach for Transportation Systems Sector[65] owners and operators to apply the tenets of the National Institute of Standards and Technology Cybersecurity Framework[66] to help reduce cyber risks. Specifically, organizations may use the implementation guidance to:

- Characterize their current cybersecurity posture
- Identify opportunities for enhancing existing cyber risk management programs
- Find existing tools, standards, and guides to support Framework implementation
- Communicate their risk management issues to internal and external stakeholders

Further, organizations that lack a formal cybersecurity risk management program could use the guidance to establish risk-based cyber priorities.[67]

While this kind of guidance is potentially of great utility to transit agencies, it does not address the significant resource constraints that most transit agencies face, and it provides neither incentive to encourage improvements in cybersecurity nor accountability for failure to do so.

DHS Programs for Public Transit Agencies

Working together, CISA and TSA have established a number of different mechanisms to provide outreach and support to transit agencies. One key program is the Cybersecurity Advisors (CSAs) Program. CSAs are DHS personnel assigned to ten regions throughout the United States, corresponding to the Federal Emergency Management Agency's (FEMA) geographic regions. They are responsible for cultivating partnerships with TSS entities—in this case, the largest transit agencies—and providing direct assistance to those entities to promote cybersecurity preparedness, risk mitigation, and incident response capabilities.[68]

CSA SERVICES

Cybersecurity Advisors offer six types of services:

1. **Cyber Preparedness:** On-site meetings to promote best practices
2. **Strategic Messaging:** Briefings, keynotes, and panel discussions to help improve cybersecurity awareness and cybersecurity posture
3. **Working Group Support:** Assisting stakeholders in existing information sharing cybersecurity initiatives
4. **Partnership Development:** Building local and regional cybersecurity private–public partnerships
5. **Cyber Assessments:**
   - Cyber Infrastructure Survey Tool (C-IST): Survey focused on over 80 cybersecurity controls in five key areas, resulting in an interactive decision support tool
   - Cyber Resilience Review (CRR): Strategic evaluation that assesses cybersecurity management capabilities
   - External Dependency Management (EDM): Assessment of the management activities and practices utilized to identify, analyze, and reduce risks arising from third parties
6. **Incident Coordination and Support:** Facilitating cyber incident response in times of increased threat, disruption, and attack.[69]

U.S. DEPARTMENT OF TRANSPORTATION

With DHS, the U.S. DOT is the TSS Co-Sector Specific Agency having responsibility for mass transit. Within U.S. DOT, FTA is the modal administration having primary responsibility.

After September 11, 2001, FTA developed security and emergency preparedness resources for U.S. transit agencies. Primary among these was FTA's *The Public Transportation System Security and Emergency Preparedness Planning Guide*[70] published in January 2003. This later evolved into the *Security and Emergency Preparedness Action Items for Transit Agencies*[71] that was used by the TSA to develop its voluntary security and emergency preparedness assessment tool, Baseline Assessment and Security Enhancement (BASE). TSA's Surface Transportation Security Inspector (STSI) activity uses the BASE checklist to work with transit agencies on a voluntary basis to complete a programmatic assessment of security and emergency preparedness programs.

The FTA and TSA revised the BASE in 2012, and those changes are reflected in the 2014 *Security and Emergency Preparedness Action Items for Transit Agencies*.[72] The main change relevant to this study was the addition of cybersecurity as a topic.[73] This change was implemented "in consultation through TSA's Mass Transit Sector Coordinating Council Chaired by the American Public Transportation Association." This addition provides approximately a page and a half of guidance that:

- Describes the transit elements at risk
- Establishes an action item to develop a cybersecurity strategy:
    - Based on risk assessment to identify critical IT assets
    - Requires development of (and updates to) written strategies and plans, including a cyber incident response plan
- Recommends training for all transit staff, including specific training for those responsible for IT assets
- Monitors information from the United States Computer Emergency Readiness Team (US-CERT)[74] and Public Transportation Information Sharing and Analysis Center (PT-ISAC)[75]
- Provides citations to a number of backup documents.[76]

On March 23, 2020, TSA published new training requirements for BASE inspectors that go into effect June 22, 2020.[77]

In 2019, the FTA issued "Frequently Asked Questions: Transit Bus Automation Policy"[78] to answer questions from stakeholders about the impact that autonomous vehicle technologies have on transit agencies. The FAQs address what transit agencies should do to develop comprehensive cybersecurity strategies and refers back to the 2014 *Security and Emergency Preparedness* document for further guidance.

In addition to the FTA, the U.S. DOT has several other modal administrations whose work impacts transit:

National Highway Traffic Safety Administration (NHTSA) leads the vehicle cybersecurity research that seeks to prevent attacks on vehicles and components.[79]

Federal Highway Administration (FHWA) leads the research that seeks to protect the nation's roadside equipment, devices, and systems. In cooperation with the National Highway Institute and other engineering organizations, FHWA developed a handbook entitled the *Federal Highway Administration Cybersecurity Handbook*.[80]

Intelligent Transportation Systems Joint Program Office (ITS JPO), while not a modal administration, is responsible for conducting research into cybersecurity mitigations for transportation technologies and promoting "security by design" for existing and emerging transportation systems.[81] This focus, while important, centers on the transportation technologies themselves, rather than the agencies' processes and procedures for acquiring and operating those technologies. The ITS JPO has established one of its goals for its 2020–2025 Strategic Plan as follows:

> ITS will be cyber-resilient. The vulnerabilities that ITS deployments create in the transportation system will be continually and systematically assessed at all levels so that risks associated with malfunction or malfeasance are mitigated to an acceptable level and resiliency plans exist and are in use.[82]

In 2018, the ITS JPO issued *Cybersecurity and Intelligent Transportation Systems: A Best Practices Guide*,[83] which presents best practices for state and local governments to develop their own ITS cybersecurity plan and penetration test program.

COROLLARY STATE AGENCIES

Every state has a corollary to DHS in some form. Most have technology hubs (e.g., office of the Chief Information or Technology Officer). These too can serve as resources for public transit agencies to support their cybersecurity efforts. The National Guard is also beginning to take an active role. Examples of state-level National Guard commissions are:

Texas Military Department, as Texas' National Guard is known, has one of the more robust state-level cyber commands in the nation, with a team of 90+ cyber resources at the ready to respond.[84]

MiC3, the Michigan civilian cyber corps.[85] Recognizing that they will never be able to match the salaries of the private sector, then-Governor Rick Snyder started the program in 2013 to recruit those with the skills and capabilities needed to protect the state's cyber resources to be called upon when needed in the event of a cyber emergency. In 2016, their mandate was expanded beyond emergencies to provide cyber support for state agencies. Immunity from liability was also added for the operation, which had 100+ volunteers.

Maryland Defense Force Cyber Security Unit supplements the cyber teams of the Maryland National Guard.[86] Created in 2010, it provides support to the Maryland Military Department and can respond alongside it in case of a cyber emergency.

California Cybersecurity Institute is a multi-agency effort to protect California through enhanced cybercrime forensics and statewide tactical response training.[87]

Cyber Collaboration Committee was established in Ohio "to determine what the state needed to improve cybersecurity and training."[88] Part of the committee's focus includes the creation of a Cyber Reserve Force, whose description is similar to the MiC3.[89]

It is imperative that public transit agencies understand the state-level resources available to them.[90]

ANCILLARY CYBERSECURITY REGULATION OF PUBLIC TRANSIT AGENCIES

Transit agencies are not subject to any specific legal or regulatory regime that mandates specific standards or actions for the implementation of a cybersecurity preparedness program.

Nonetheless, transit agencies, like most other entities, are governed by a patchwork of legislation and regulations that do impose some cybersecurity rules. For example:

- To the extent transit agencies process payments, they are subject to cybersecurity rules that govern the financial sector (usually imposed by contracts from the banks or credit card companies with whom they partner).

- Similarly, in handling customer data (including payment information), transit agencies must comply with relevant state privacy rules and various breach notification requirements that may be triggered by a data loss.

- Transit agencies are also subject to the broad reach of the Federal Trade Commission (FTC), which has the authority to levy fines and other penalties against companies that engage in unfair or deceptive trade practices.

None of these various elements amounts to a regulatory regime that even comes close to establishing a standard of practice that transit agencies could use as a guide in implementing a cybersecurity preparedness program. While DHS and some of the corollary state agencies have provided assistance to transit agencies, much of the critical guidance comes from within the transit industry.

KEY INDUSTRY ASSOCIATIONS SUPPORTING TRANSIT[91]

As with many aspects of the U.S. economy, much of the onus for ensuring effective management of cybersecurity risks rests within the industry itself. Here, APTA ably serves

the needs of the public transit industry. APTA is a nonprofit, international trade association with more than 1,500 public and private sector members. APTA provides a broad range of services to its members that include advocacy and policy, standards, guidance and best practices, training, research, and technical support.

There are other trade associations that represent segments of APTA's membership, such as the American Association of Highway and Transportation Officials (AASHTO), the Intelligent Transportation Society of America (ITS America), the American Bus Association (ABA), and the International Association of Public Transport (UITP).

APTA has been providing its members with guidance on cybersecurity for the past decade. That guidance has come primarily through its Security Standards Policy and Planning committee and its working groups on security and emergency management standards. The aforementioned committee is composed of representatives from a number of prominent transit organizations and businesses and is organized into several working groups. One working group is the Enterprise Cyber Security working group, which focuses specifically on cybersecurity. In 2014, this group published Recommended Practice "Cybersecurity Considerations for Public Transit," providing a good overview of materials available to transit operators; this Recommended Practice in particular establishes considerations for public sector chief information officers (CIO) interested in developing cybersecurity strategies for their organizations.[92] This document also references earlier guidance that APTA provided CIOs, including "Securing Control and Communications Systems in the Transit Environment," Part 1 and Part II.[93]

AASHTO's purpose is to meet the needs of the state and territorial departments of transportation (DOTs). State DOTs have multimodal responsibility, and as such, AASHTO has a Council on Public Transit. This Council "develops legislative, policy, and program recommendations related to all forms of passenger public transportation services."[94]

The Council also supports the Multi-State Transit Technical Assistance Program (MTAP), the primary purpose of which is to provide technical assistance to help states implement FTA programs, to provide feedback to FTA on implementation issues, and to create a professional network for sharing best practices.[95]

Information abounds for public transit agencies wanting to develop their own cybersecurity preparedness programs; however, few prescriptions exist. Regulations and requirements are even fewer, aside from those regulations that cross over to other industries with more robust regulatory and compliance frameworks in place, despite public transit agencies being labeled a critical infrastructure element for U.S. security.

V. KEY FINDINGS

The survey findings demonstrate that many transit agencies do not fully appreciate the risks posed by cybersecurity vulnerabilities nor the necessity to prepare for the inevitable attempts at a breach. Transit, however, is not unique in this regard. To provide perspective, the section draws comparison to the financial industry. Given both the level of the threat and the long history in dealing with such threats, understanding the preparation and the resources allocated to this matter in the financial industry can help inform resourcing decisions for transit. Throughout the presentation of findings, the authors provide anecdotes from the financial sector to help frame what is needed in public transit.

Funding alone is not enough to address cybersecurity risks. The root challenge for any organization is marshalling the nonmonetary as well as monetary resources to develop an effective cybersecurity program. This cannot be done without a mix of resources, from executive and board-level involvement to effective hiring of cybersecurity expertise and alignment with the overall strategy of the organization. A key lesson from other industries is that cybersecurity preparedness does not happen in a vacuum. Systems, policies, procedures, and other plans must be developed and iterated as new data, information, and threats are discovered.

The survey findings present a significant cause for concern. Despite the substantial focus that the industry has placed on cybersecurity education and preparedness over the past decade, many transit operators remain ill prepared for the cybersecurity challenges they are facing and are likely to face in the future. As the industry is learning with COVID-19, mitigation tactics can only get you so far; the key question is not whether an incident will occur but when. Far too many agencies have not implemented adequate cybersecurity measures and are not ready to respond to a cyber incident.

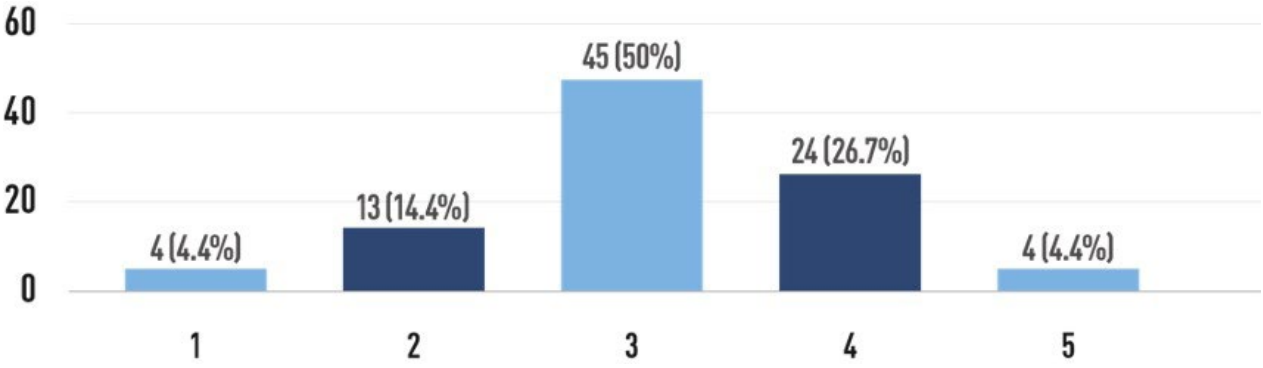
FINDING: MANY AGENCIES DO NOT HAVE AN ACCURATE SENSE OF THEIR CYBERSECURITY PREPAREDNESS

- 81% of agencies that responded believe they are prepared to manage and defend against cybersecurity threats, and;
- 73% feel they have access to information that helps them implement their cybersecurity preparedness program.

Yet…

- Only 60% actually have a cybersecurity preparedness program;
- 43% do not believe they have the resources necessary for cybersecurity preparedness; and
- Only 47% audit their cybersecurity program at least once per year.

Figure 11 shows that 81% of the organizations that responded to the online survey reported being adequately prepared to manage and defend against cybersecurity threats. Yet Figure 12 shows that only 60% of the agencies have a cybersecurity policy in place. Given the authors' review of practices in other industries, it seems highly unlikely that an agency could be prepared to defend against a cybersecurity threat without having a documented cybersecurity policy.



1 = Not prepared at all.
5 = Very prepared.

Figure 11. How Prepared Would You Say Your Organization is in Managing and Defending Against Cybersecurity Threats?

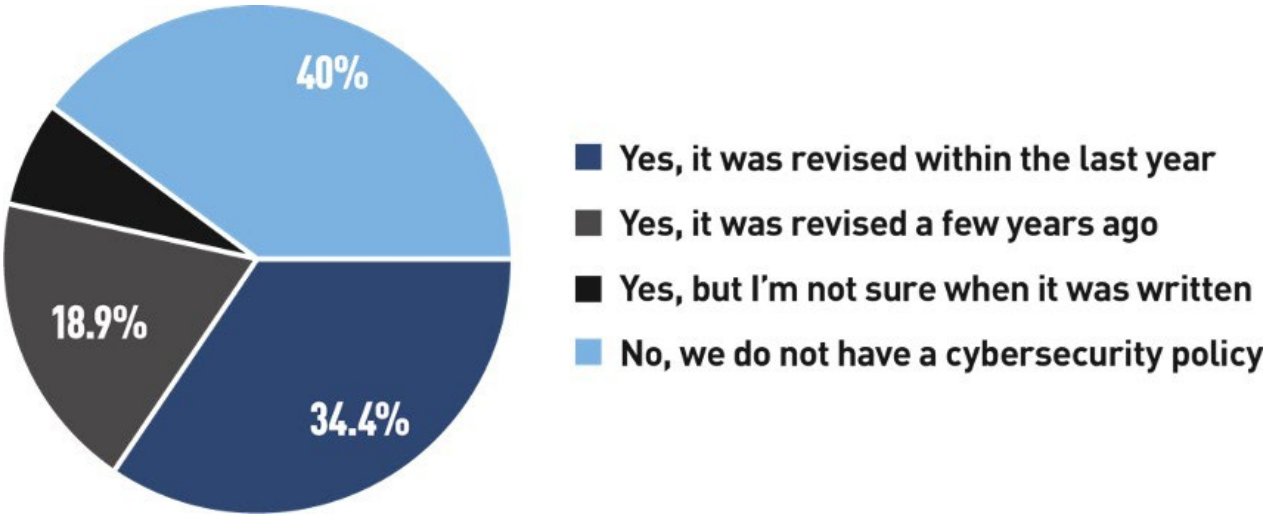
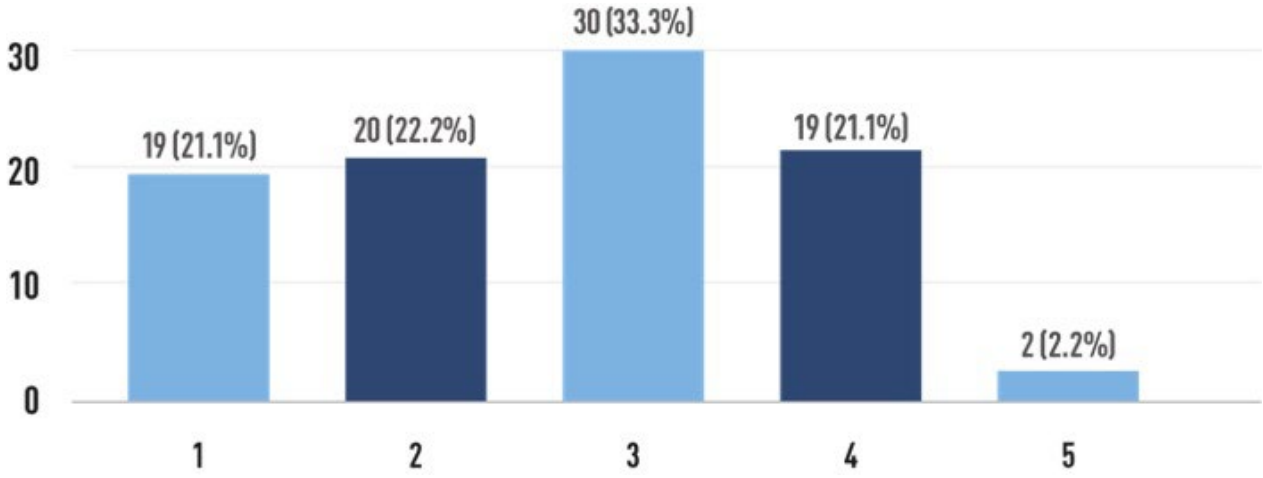


Figure 12. Do You Have a Documented Cybersecurity Policy? If So, How Often is it Revised?

Despite the support activity from both industry groups and government agencies discussed earlier in Section IV, Existing Cybersecurity Guidance for Transit, most oral interviewees reported lacking the resources needed to effectively prepare for and respond to a cyber incident. This finding was supported by survey data. As Figure 13 illustrates, 39 of the respondents (43%) said they do not have the resources they need to be prepared. Only two agencies felt strongly that they have the resources needed for cybersecurity preparedness, and one of those is a small agency (<$10M in operating expenses).

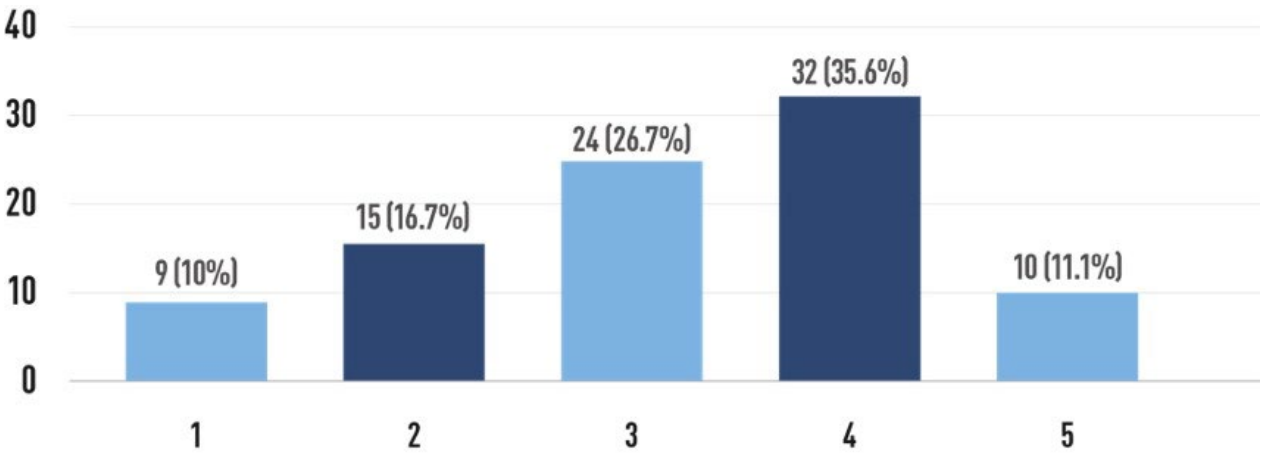
Oral interviewees attributed this lack of resources to a lack of prioritization by their leadership. Several brought concerns directly to the attention of their CEO or their Board, and even then they had limited success obtaining what they believed was necessary. One interviewee suggested that resources for cybersecurity only became available after a major incident. Another leveraged an outside audit (e.g., DHS CSA review, FTA's Triennial Review,[96] cybersecurity incident insurance) to highlight the potential liability to her Board and access greater support.



1 = I do not have what I need to be prepared.
5 = I have everything I need to be prepared.

Figure 13. Do You Have the Resources (e.g., Funding, Training, Other Support) You Need for Cybersecurity Preparedness?

Figure 14 shows that access to information does not appear to be a major challenge for the agencies that responded; only 24 agencies (27%) reported lacking access to information and guidance that helps them implement their cybersecurity preparedness program. There is a material amount of useful and effective information available to assist transit agencies implementing a cybersecurity program. This statement is affirmed by the literature review. The challenge centers on having the resources to take advantage of the information available, and developing a specific plan for each agency's unique needs.



1 = No, I do not have access to information and guidance that helps me.
5 = Yes, I have access to all information and guidance I need.

Figure 14. Do You Have Access to Information and Guidance That Helps You Implement Your Cybersecurity Preparedness Program?

FDIC Cyber Challenge

Like transit, the financial services industry is made up of a patchwork of large and small players. To help smaller community banks, the Federal Deposit Insurance Corporation (FDIC), one of the primary regulators of the U.S. banking system, created the "Cyber Challenge Community Bank Cyber Exercise" program. The agency has developed and now maintains nine different scenarios for community banks to consider when assessing their cybersecurity preparedness.

The Cyber Challenge is designed to help financial institution management and staff discuss events that may present operational risks and consider ways to mitigate them. It can provide useful information about an institution's preparedness and identify opportunities to strengthen the bank's resilience to operational risk.[97]

According to the survey, just over 60% of responding agencies audit their cybersecurity program (see Figure 15). However, of those, only two-thirds (46% of all respondents) perform this audit annually; the remaining agencies audit their cybersecurity preparedness on an as-needed basis (see Figure 16). As discussed above, external audits can be effective in drawing the attention of CEOs and Board members to deficiencies in cybersecurity preparedness.

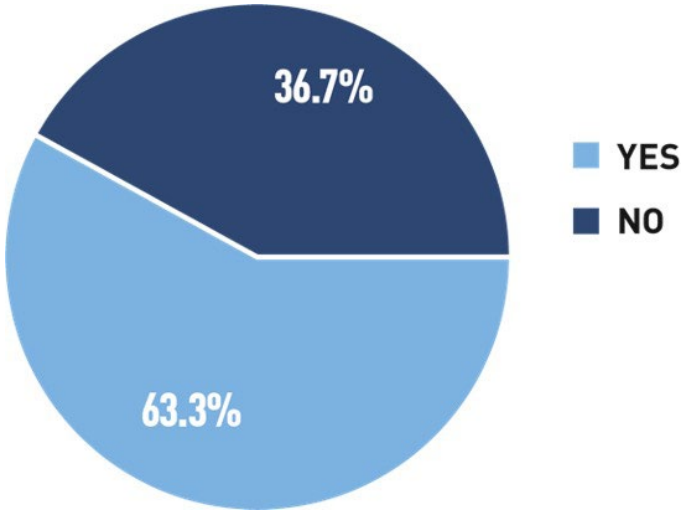


Figure 15. Is There a Process (Either Internal or External to Your Organization) That Audits Your Cybersecurity Preparedness Program or Establishes Some Other Accountability Mechanism for That Program?

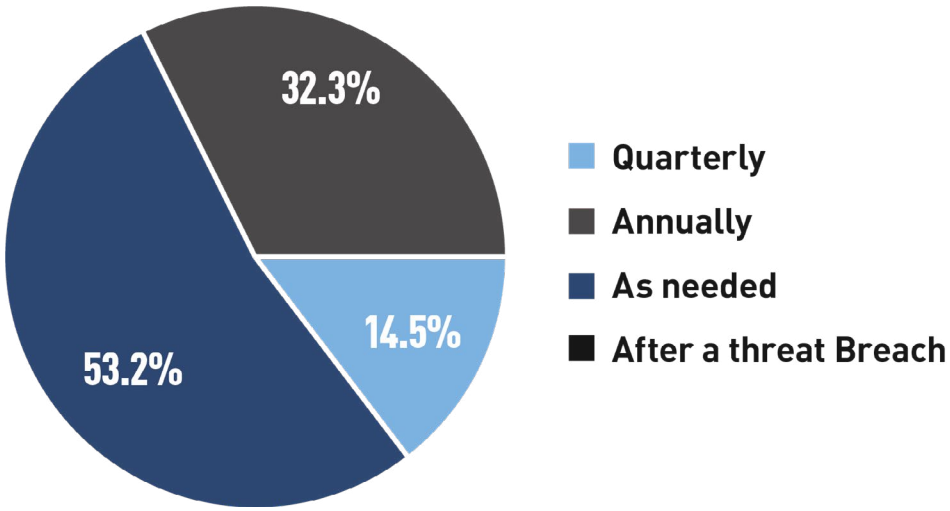


Figure 16. If Yes, How Frequent is the Audit?

The agencies surveyed claim they have not had many cybersecurity incidents. Of the 90 agencies surveyed, only 20 agencies (22%) admitted to having had a cybersecurity incident where more than 1,000 records were breached, over $10K in losses were incurred, or an operations system was down for more than one hour. These results seem highly suspect. A forthcoming Transportation Research Board NCHRP Report "*Security 101: A Physical and Cybersecurity Primer for Transportation Agencies*" observes that:

> (T)he relatively few number of catastrophic incidents in transportation to date has resulted in a false sense of security within the transportation sector. Recent research estimated that on the physical security side as many as 75% of security breaches go unreported. In terms of cyber much less is known about prospective breach percentages,

but there is little reason to believe that the numbers are any better for cyber incidents. What is known is that the ease of compromise of transportation cyber systems is becoming more and more evident, and the likelihood of new or more significant events is increasing along with the per event costs of cyber incidents and cyber-crime.[98]

FINDING: MOST AGENCIES DO NOT HAVE LOG MAINTENANCE SCHEDULES WHICH SATISFY A BASIC TENET OF CYBERSECURITY PREPAREDNESS

- 51% of agencies that responded do not retain their log data for a year or more—one of the most basic requirements for cybersecurity preparedness
- 12% of agencies surveyed do not retain their logs at all

Many agencies fail to implement one of the most fundamental technical cybersecurity measures: collecting, retaining, and analyzing system log data. Often, when an incident occurs, it is identified weeks or even months after it originated. Retaining logs is a critical source of evidence necessary to figure out when the breach occurred and what systems were affected. Just over half of agencies that responded retain their logs for a year or more—the minimum duration cybersecurity experts recommend retaining logs.[99]

Log maintenance is a complicated issue, and every organization should have a formal log maintenance plan that speaks to each type of log being captured, how it is retained, for how long, and how it is disposed of.[100] Beyond mere retention of a log, the failure to analyze that log data is the primary reason intrusions go undetected for months or years after they have occurred. The evidence of the intrusion may sit languishing in unexamined log files.[101]

FINDING: MOST AGENCIES DO NOT HAVE MANY OF THE BASIC POLICIES AND PROCEDURES IN PLACE TO RESPOND IN THE EVENT OF AN INCIDENT

- 42% don’t have an incident response plan; of those that have one, over half have not had a drill in over a year
- 36% do not have a disaster recovery plan
- 53% do not have a continuity in operations plan
- 58% do not have a business continuity plan
- 67% do not have a crisis communications plan

Transit agencies have failed to adopt basic plans that would be necessary in the event of an incident. Agencies need to plan for incident response in parallel to taking steps to lessen its probability. Of the 90 agencies that responded, 52 agencies have a documented incident response plan, and of those, only 23 had a drill within the last year (see Figure 17). This suggests that, to the extent that an agency knows that an incident has occurred,

confusion and challenges in communication, among other issues, may hinder response effectiveness for the agency.

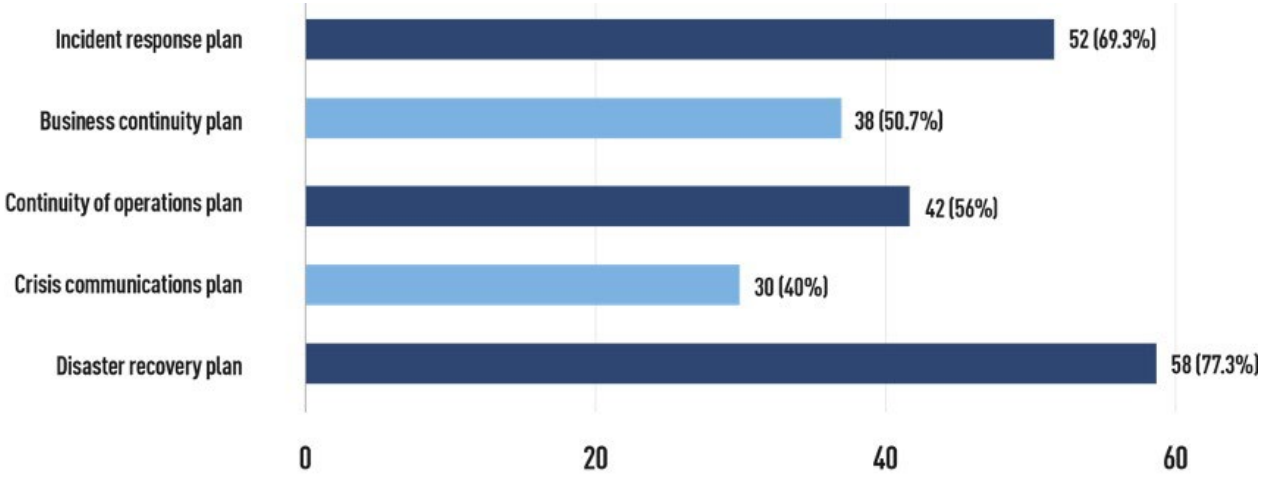


Figure 17. Do You Have a _____ Plan (Check All Plans That Apply)?

NIST 800-100, *Information Security Handbook: A Guide for Managers*, one of the basic NIST Guidance documents, provides a "*Seven-Step IT Contingency Planning Process*"[102] that provides transit agencies a process that they can use to quickly identify a security incident and take appropriate steps to recover from it. APTA, in its Recommended Practice "Cybersecurity Considerations for Public Transit," summarizes the suite of plans an organization should use "to properly prepare response, recovery and continuity activities for disruptions affecting the organization's information systems, mission/business processes, personnel and facilities."[103] These documents include an Incident Response Plan, Business Continuity Plan, Continuity of Operations Plan, Crisis Communications Plan, and Disaster Recovery Plan.

FINDING: MANY AGENCIES LACK THE STAFF AND THE NECESSARY SKILLS OR TRAINING TO ADDRESS CYBERSECURITY THREATS

- Only 41% of agencies provide at least annual cybersecurity training for staff
- Cybersecurity staffing levels are low, even among large agencies or agencies that have suffered an incident, relative to other industries

Since the internet came of age and software became a more critical aspect of any organization's execution, the role of the cybersecurity specialist has evolved. Once relegated to the basement, cybersecurity experts have "grown up," moved from the basement to the office, and are now seated at the table with senior leadership. Many transit agencies have not kept pace in hiring cybersecurity staff nor have they conducted the necessary training to ensure the organization has the skills necessary to address the threat landscape. Agency leadership needs cybersecurity expertise at the table, ready to support them with both strategic and operational decisions in real time.

The prioritization among transit agencies of resourcing cybersecurity needs appears limited. Through oral interviews, several suggested that the successes they have had in developing their cybersecurity programs have rested on their obtaining experience from other industries. One such interviewee remarked, "We are the outlier. We have a full-scale program. [We have] people focused directly on cybersecurity with two focused just on supply chain issues."[104] Agencies should look to bring in cybersecurity expertise from other industries, in addition to attempting to develop talent from within.

Only 38 of the 90 survey respondents have certified cybersecurity specialists on staff, and there is no consensus within the industry on which certification to require among potential new hires. Agreement among transit professionals and industry experts about the value of, and need for, specific cybersecurity certifications would be beneficial for all.

Table 2. Certifications Held by Staff of Surveyed Agencies

Agency Count	Certification
21 (23%)	Certified Information Security Professional (CISSP), a certification provided by the Information Security Consortium (ISC)[2].[105]
8 (9%)	Certified Ethical Hacker (CEH), offered by the International Council of eCommerce Consultants (EC-Council)[106]
6 (7%)	Certified Information Systems Auditor

Interestingly, from oral interviews, the authors learned that the transit cybersecurity professionals that were recruited from other industries have sought each other out and maintain regular, informal communications. While this likely assists those involved in cybersecurity preparedness, these individuals have the least need for these informal networks.

Survey results show that headcount dedicated to cybersecurity does not correlate with either agency size or with whether the agency reported having suffered an incident as we would have anticipated. For those leaders interviewed who had developed a robust cybersecurity team and program, the driving force behind their ability to build a dedicated cybersecurity staff was that they had experienced a significant cyber incident. However, the authors did not find corroboration for this anecdotal evidence in the digital survey data.

Figure 18 shows that of the 35 agencies with no personnel dedicated to cybersecurity, 17 are large or extra-large (>$30M in operating expenses). Among the 30 extra-large agencies surveyed (>$100M in operating expenses), only six have five or more personnel dedicated to cybersecurity. Three extra-large agencies have no personnel dedicated to cybersecurity.

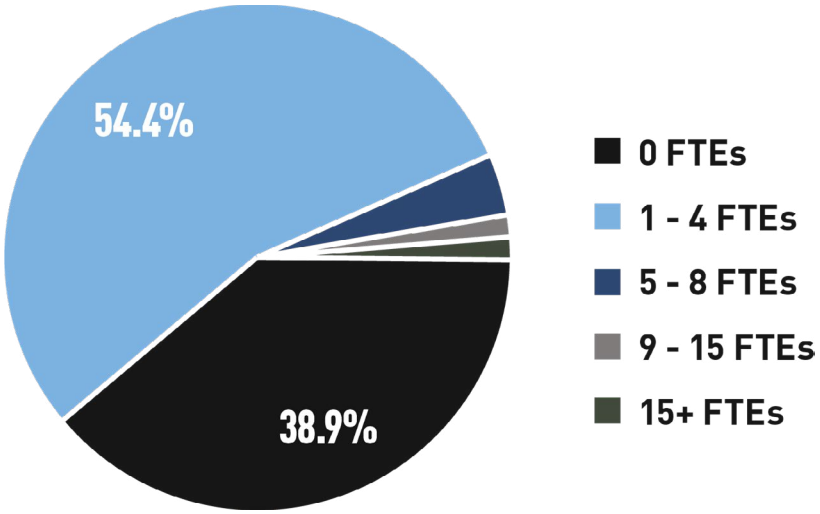


Figure 18. What is Your Internal Headcount Dedicated to Cybersecurity Preparedness? (In Full Time Equivalents (FTE))

Similarly, having had a cyber incident does not necessarily drive the size of the cybersecurity staff. Among the 20 agencies that reported having suffered an incident, four have no personnel dedicated to cybersecurity, and only one has more than five—this despite the fact that 17 of the 20 agencies are large or extra-large relative to operating expenses.

How Much is Enough?

No hard data exist for how much public transit agencies should invest in cybersecurity staff, software, and services; however, there are a few "rules of thumb" available from the private sector. One rule used by a public transit agency cybersecurity executive interviewed is to have one dedicated full time equivalent (FTE) focused on cybersecurity per 500 employees.[107] Among the agencies surveyed for this study, the majority fall within this rule of thumb at 53%.

Figure 19 illustrates that financial institutions spend an average of 0.3% of revenue and 10% of their IT budget on cybersecurity, according to numbers tallied by the consulting firm Deloitte. "That works out to about $2,300 per employee, across the 96 financial firms that took part in the Deloitte study, according to American Banker."[108]

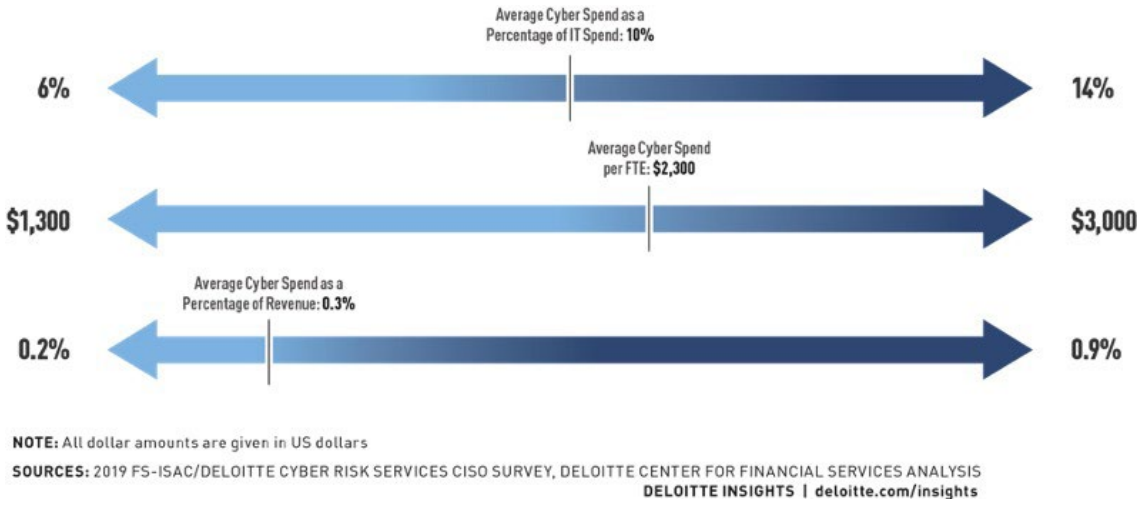


Figure 19. Average Cybersecurity Spending Range[109]

For reference, among survey respondents, public transit agencies have an average cyber budget of $1,490 per employee, with a min (max) of $30 ($3,600) per employee.[110] From the same survey, the average cyber budget is 2.8% of operating expenses, with a min (max) of 0.02% (2.7%).[111] The averages are in range, but the variability among agencies is significant. The authors were not able to observe a common thread among the survey data as to why some agencies invest in cybersecurity and others do not. One inference from oral interviews suggests agencies that recruit cybersecurity specialists from other industries are more effective in developing a cybersecurity program on par with the rules of thumb described above.

NuHarbor Security, a cybersecurity services vendor, suggests that once an enterprise reaches four internal cybersecurity-focused staff, they must hire a "people manager" to ensure the unique needs of this team are met and their interests are represented within the organization. Organizations with more than 5,000 employees should have a Chief Information Security Officer on the senior leadership team to ensure the interests of information security are appropriately represented among strategic decisions.[112]

For the staff that transit agencies do hire, most do not provide cybersecurity training, provide it only upon hire, provide it irregularly, or provide it on a voluntary basis only. Figure 20 shows that of the 90 agencies that responded to the survey, only 37 of them (41%) provide training at least annually.

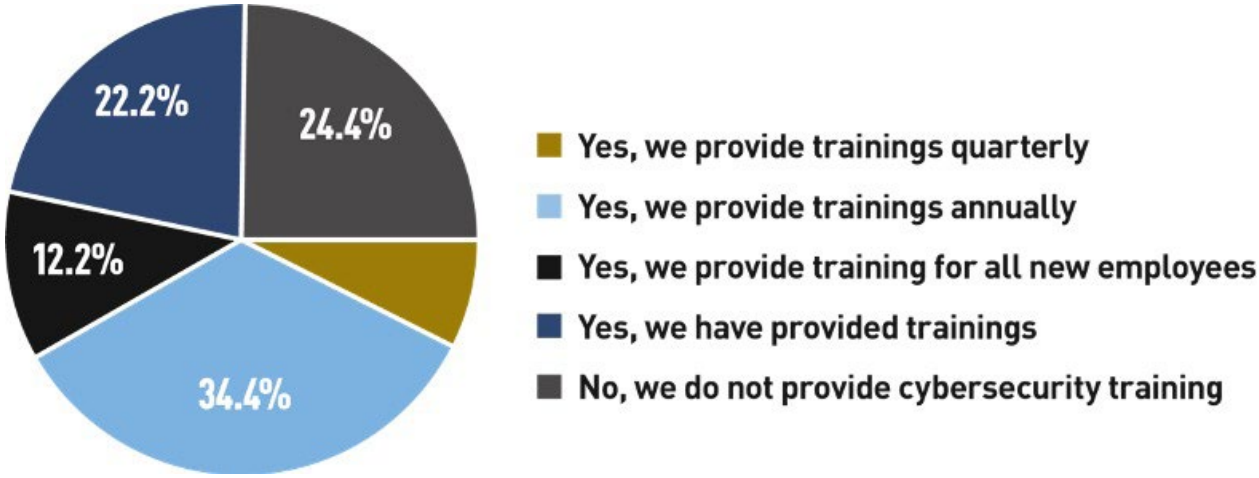


Figure 20. Do You Have Regular Cybersecurity Training? How Often? Who is Trained?

Of those that do not provide training with regularity, a large majority blame the lack of resources. The authors infer that, given the ample opportunities that exist to obtain cybersecurity training materials and modules, the limiting factor is more a function of underestimating and de-prioritizing cyber threats rather than fiscal or other resource constraints. As noted in the Introduction and then again in the discussion of association support, APTA has made cybersecurity training a high priority for its membership. In addition to routinely programming speakers and educational sessions on cybersecurity at its various meetings, APTA invested in a high-quality training video developed for executives called "Cybersecurity Fundamentals for Executives."[113] Since its launch at the APTA Annual Meeting in October, 2019 this training video has been accessed more than 5,000 times.

FINDING: AGENCIES ARE ENGAGING VENDORS FOR CYBERSECURITY SUPPORT, BUT THEY ARE NOT ALWAYS PROTECTING THEMSELVES OR THEIR CUSTOMERS WITH APPROPRIATE CYBERSECURITY LANGUAGE

- 84% have engaged at least one vendor to provide cybersecurity software, tools, and support

- Only 38% include standard clauses in their contracts to impose cybersecurity requirements on all their vendors

Most agencies have taken measures to outsource some key cybersecurity functions to vendors, as shown in Figure 21; 75 of the respondents (84%) have engaged at least one vendor to provide cybersecurity tools, software, and support.

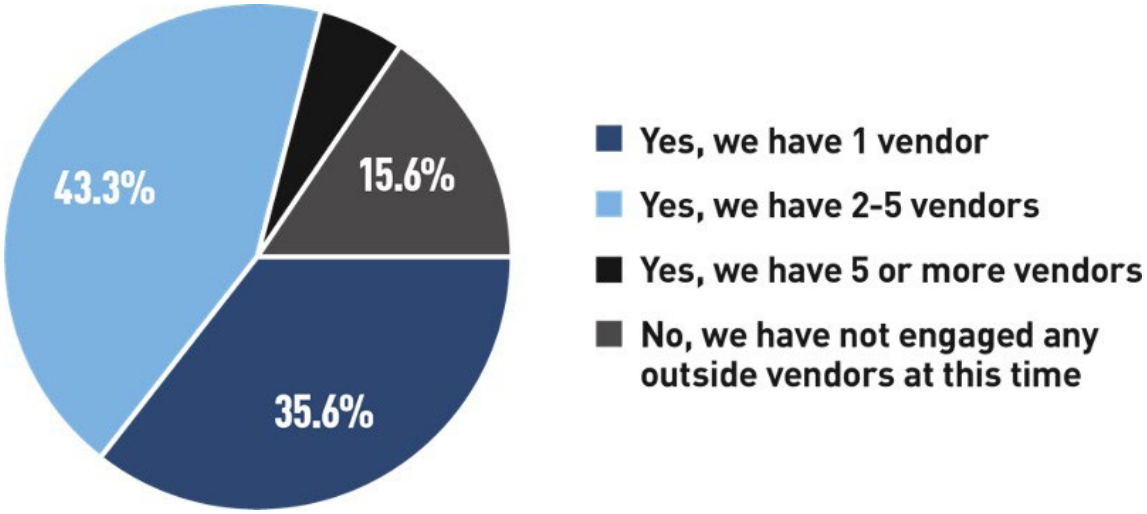


Figure 21. Have You Engaged Outside Vendors to Provide Tools, Software, and Support to Assist With Cybersecurity Preparedness?

Many leverage vendors to off-load the risk and expense of managing data covered by PCI requirements, such as credit card data and processing. By having the vendor manage these applications (and data), the transit agency can contractually require that the vendor maintain state-of-the-art cyber protections. Of the 90 agencies surveyed, 76 of them (84%) use a vendor to process and store customer payment information.

However, it appears that more work needs to be done among agencies to hold their vendors accountable for cybersecurity readiness. Only 34 of the respondents (38%) have standard clauses in their contracts related to cybersecurity: see Figure 22. An agency's cyber readiness is only as strong as its weakest link. The inability to hold vendors accountable for their cybersecurity preparedness is a key weakness for public transit agencies.

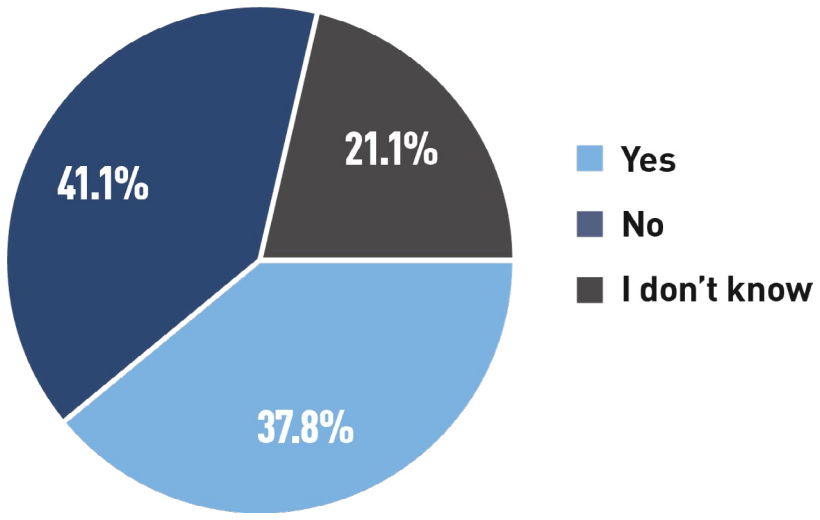


Figure 22. Do You Have Standard Clauses in Your Vendor Contracts Related to Cybersecurity?

The oral and digital surveys are informative in conjunction with the literature review. If an agency has the time and resources, there is an abundance of information on cybersecurity risks and tools available to transit authorities. Many transit agencies are aware of the risks posed and have taken some actions to protect themselves and some agencies have or are in the process of putting robust cybersecurity programs in place. Those that have the most robust programs tend to be the largest agencies with the most risk from a public safety perspective but also the most federal resources available to them to help address those risks.

For the majority of transit agencies, cybersecurity will remain one of many important competing demands for limited resources. Until, and unless, the Federal government makes cybersecurity a priority for transit agencies; provides them with the resources necessary to establish and maintain solid cybersecurity programs; and provides them with clear guidance on what constitutes a “solid” cybersecurity program, most agencies will continue to do the best that they can. When resources become available, they will avail themselves. When clear guidance becomes available, they will avail themselves of it, and as they become more sophisticated over time they will do their best to transfer as much responsibility as possible to third parties. When there is a cybersecurity incident they will be forced to reallocate their limited resources to address this critical priority.

VI. POLICY RECOMMENDATIONS

To support the findings described in the previous section, the authors propose the following policy recommendations.

EXECUTIVE BRANCH

- DHS and U.S. DOT, the TSS Co-Sector Specific Agencies for transit, working with input from APTA and other industry organizations, should promulgate a set of minimum cybersecurity standards and cybersecurity assessment tools and determine how they should best be developed, managed, and implemented.

- DHS and U.S. DOT should provide technical guidance to transit agencies on the collection, retention, and assessment of system logs.

- FTA, working with DHS, should create an attestation program, whereby transit CEOs are required to attest that their organization has met the minimum cybersecurity standards established above prior to receiving federal funds.

- FTA, working with DHS and other relevant federal agencies, should require that transit agencies either outsource management of payment data to PCI-compliant vendors, or require that their CEO attest that they are PCI-compliant prior to receiving federal funds.

LEGISLATURE

- Congress should increase funding to DHS and U.S. DOT to develop and promulgate a set of minimal cybersecurity standards and tools and for their promotion.

- Congress should increase formula grant funding to transit agencies to ensure that they have sufficient resources to meet the minimal cybersecurity standards established above.

- Congress should ensure through its oversight powers that U.S. DOT and DHS work together to improve cybersecurity preparedness within the TSS.

INDUSTRY/ASSOCIATION

- APTA, working with other stakeholders, should develop a clearinghouse for cybersecurity best practices, in particular for small and medium transit operations.

- Transit Operators should develop an individualized cybersecurity plan that takes advantage of the best practices identified above and highlighted throughout this study.

- APTA, working with other stakeholders, should create minimum guidelines for cybersecurity audits.

- Transit Operators should conduct a periodic cybersecurity audit and address the shortcomings identified in that audit in a timely manner.

- APTA, working with other stakeholders, should develop model cybersecurity contract language for agencies to integrate into their vendor contracts.

- Transit Operators should ensure all vendor contracts include standard cybersecurity contract language. Transit Operators should conduct an audit of all external contracts and ensure that the contracts have current, robust, cybersecurity contract language in them protecting the Transit Operator.

- APTA, working with other stakeholders, should develop a model Incident Response Plan, Business Continuity Plan, Continuity of Operations Plan, Crisis Communications Plan, and Disaster Recovery Plan that can be tailored to meet the needs of public transit organizations of varying sizes and needs.

- Transit Operators should document their security response plans respective of industry best practices for their agency size and other variables. Transit Operators should regularly conduct drills to ensure that they have the right plans in place and that the organization is able to effectively react to incidents.

- APTA, working with other stakeholders, should continue to develop cybersecurity training modules and certificates. In doing so it should take advantage of the guidance developed by TSS, CSAs and others.

- Transit Operators should ensure that every employee receives the appropriate level of cybersecurity training at least annually.

The cybersecurity threat to public transit operations is real. This is not a new observation, as many before have tried to emphasize the need to address this threat. The resources and knowledge are available; what is lacking is the focus at all levels. Mitigating this threat and reducing its impact requires concerted, coordinated effort among policy makers, industry representatives and public transit leadership. The recommendations above seek to incentivize the respective stakeholders to work together to make our public transit systems more safe, secure, and resilient.

APPENDIX A: ORAL INTERVIEW GUIDE FOR TRANSIT OPERATORS

NOTE: We will only use your name or organization if you give us explicit permission.

Name:

Organization:

Job title:

Email:

Phone:

Please describe your organization's cybersecurity responsibilities:

What resources are allocated to cybersecurity in your organization?

Budget:

Internal dollars:

External dollars:

Headcount (in full-time equivalents):

Are they sufficient?

What else do you need?

What percentage of your budget is this?

Who is responsible for cybersecurity within your organization?

What is your role?

Do you have a Chief Information Security Officer? A Chief Privacy Officer? A Chief Compliance Officer?

Has your organization suffered from an attack? What type? How often? Have you conducted any research to determine whether your organization has suffered an attack that you weren't otherwise aware of?

Do you have a documented cybersecurity policy? If so, who within your organization is familiar with its contents? When was it put into place?

In creating your cybersecurity policy, have you applied the principles and guidance from the NIST Cybersecurity Framework (or a different risk-management framework)?

Does your cybersecurity plan govern the entirety of your information management process (e.g., establishment of business requirements, procurement, operations, maintenance, disposal)?

Do you conduct cybersecurity training? If so, for whom and how often?

Do you have cybersecurity insurance? If so, what are the terms/costs?

Do you have an incident response plan (IRP)? Was that plan drafted by someone within your organization? Have you ever rehearsed that plan?

Where do you get your cyber threat information? Is your organization a member of an entity that shares cybersecurity information (e.g., the Public Transportation Information Sharing and Analysis Center)?

Do you have contractual provisions associated with cybersecurity that you require?

Can we get copies of these documents? Do you have a mechanism for auditing whether those vendors are meeting the requirements?

Do others outside your organization engage on cybersecurity in regards to your operations (e.g., an auditor, consultant, law firm, city)? Do you have a contractual relationship with a third-party forensic investigator who can assist in the event of a data breach?

Do you have SCADA systems in your network? How are they connected to/isolated from your business network? Are they remotely accessible?

Do you maintain payment processing information? If so, do you adhere to the Payment Card Industry Data Security Standard (PCI DSS)?

Are you receiving direction / requirements / process guidance from the city's CISO or other? Do you report out on your cybersecurity policies / practices to any person, entity or organization?

Do you feel that your organization understands the threat that cybersecurity presents to the transit industry?

If not, why not?

What would it take to improve your understanding?

Do you feel that your organization is doing everything that it can to prevent a cybersecurity attack on the transit industry?

What more could it be doing?

What do you need to do this?

What role do the various branches of the Administration play in establishing standards and best practices for the transit industry?

What role should they play?

What would it take for them to play these roles?

Does the Administration have an adequate understanding of the risks that cybersecurity presents to the transit industry?

Has the Administration allocated sufficient resources to the correct organizations?

If no, what should the allocation be?

Has the Administration placed sufficient priority on cybersecurity?

What role does Congress play in establishing standards and best practices for the transit industry?

What role should it play?

Is cybersecurity a sufficient priority for Congress?

Does Congress have an adequate understanding of the risks that cybersecurity presents to the transit industry?

What role does APTA and other industry organizations play in establishing standards and best practices for the transit industry?

What role should they play?

Is cybersecurity a sufficient priority for these groups?

Do they have a sufficient understanding of the risk that cybersecurity presents to the transit industry?

APPENDIX B: ORAL INTERVIEW GUIDE FOR NON-TRANSIT OPERATORS

NOTE: We will only use your name or organization if you give us explicit permission.

Name:

Organization:

Job title:

Email:

Phone:

Organization type:

Organization's cybersecurity responsibilities:

What resources are allocated to cybersecurity in your organization?

Budget (not including:

Internal dollars:

External dollars:

Headcount (in full-time equivalents):

Are they sufficient?

What else do you need?

What percentage of the organization's budget is this?

Who has lead responsibility for issues related to cybersecurity within your organization?

What is your role?

Has your organization produced documents applicable to transit cybersecurity?

If so, who within your organization is familiar with their contents?

When were they put into place? Have they been updated?

Do you think they are sufficient? If not, why not?

Can we get copies?

Do you feel that your organization understands the threat that cybersecurity presents to the transit industry?

If not, why not?

What would it take to improve your understanding?

Do you feel that your organization is doing everything that it can to prevent a cybersecurity attack on the transit industry?

What more could it be doing?

What do you need to do this?

What role do the various branches of the Administration play in establishing standards and best practices for the transit industry?

What role should they play?

What would it take for them to play these roles?

Does the Administration have an adequate understanding of the risks that cybersecurity presents to the transit industry?

Has the Administration allocated sufficient resources to the correct organizations?

If no, what should the allocation be?

Has the Administration placed sufficient priority on cybersecurity?

What role does Congress play in establishing standards and best practices for the transit industry?

What role should it play?

Is cybersecurity a sufficient priority for Congress?

Does Congress have an adequate understanding of the risks that cybersecurity presents to the transit industry?

What role does APTA and other industry organizations play in establishing standards and best practices for the transit industry?

What role should they play?

Is cybersecurity a sufficient priority for these groups?

Do they have a sufficient understanding of the risk that cybersecurity presents to the transit industry?

APPENDIX C: ORAL INTERVIEW GUIDE, CAPITOL HILL

NOTE: We will only use your name or organization if you give us explicit permission.

Name:

Organization:

Job title:

Email:

Phone:

We understand that your office has been engaged in cybersecurity issues, particularly those involving the transit industry, and we would like to ask you some questions related to your offices' engagement.

Why has your office become engaged in this issue? [hint: member serves on committee of relevant jurisdiction; large scale transit operations in the district, recent cybersecurity attack in the community or state.]

What is your role in that engagement?

Do you feel that Congress understands the threat that cybersecurity presents to the transit industry?

If not, why not?

What would it take to improve its understanding?

Do you feel that the House/the Senate/the Committee on which your boss serves is doing everything that it can to address cybersecurity in the transit industry?

What more could it be doing?

What do you need to do this?

Does Congress have an adequate understanding of the risks that cybersecurity presents to the transit industry?

What role should Congress play in establishing standards and best practices for the transit industry?

Is cybersecurity a sufficient priority for Congress?

Would you like to add anything that would aid us in better understanding your senators'/

members' views on cybersecurity in transit?

Now I would like to ask you a few questions about other participants in this issue:

What role do the various branches of the Administration play in establishing standards and best practices for the transit industry?

What role should they play?

What would it take for them to play these roles?

Has the Administration allocated sufficient resources to the correct organizations?

If no, what should the allocation be?

Has the Administration placed sufficient priority on cybersecurity?

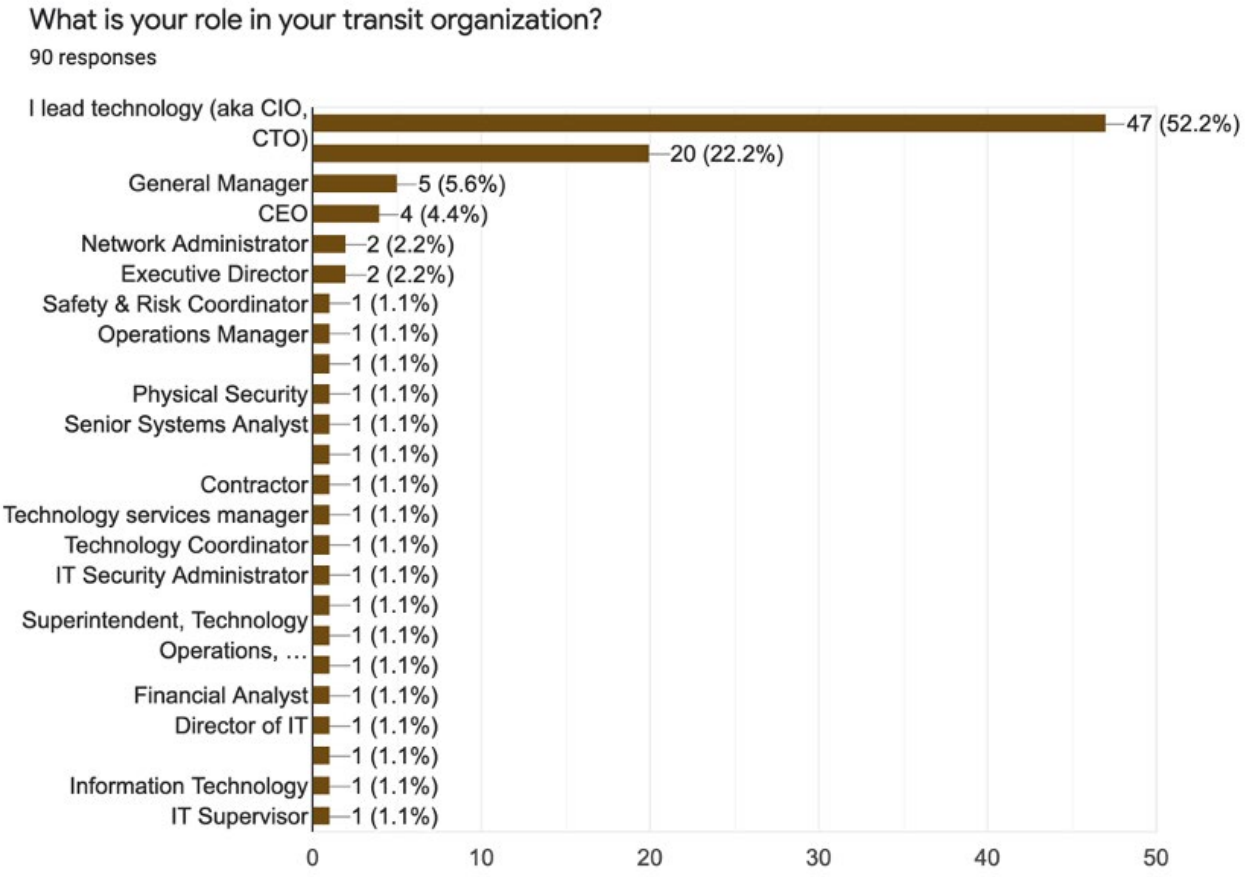
Does the Administration have an adequate understanding of the risks that cybersecurity presents to the transit industry?

What do you see as the role for non-governmental organizations such as trade associations in this issue?

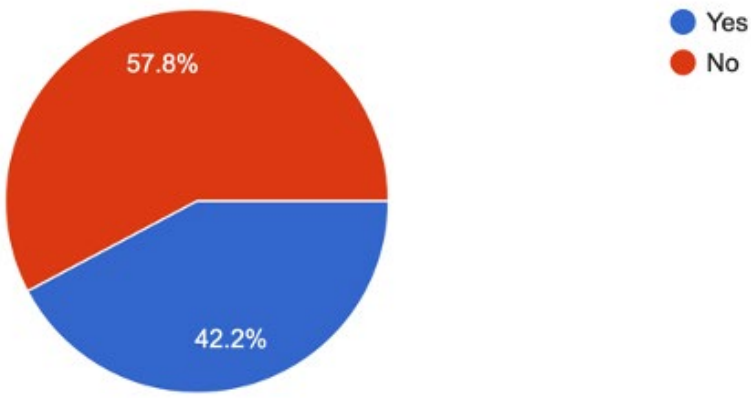
APPENDIX D: MTI DIGITAL SURVEY AND DIGITAL SURVEY RESPONSES

The Mineta Transportation Institute at San José State University has commissioned a study to investigate the extent to which the transit industry is ready for the cyber revolution and to make policy recommendations to enhance surface transit cyber preparedness.

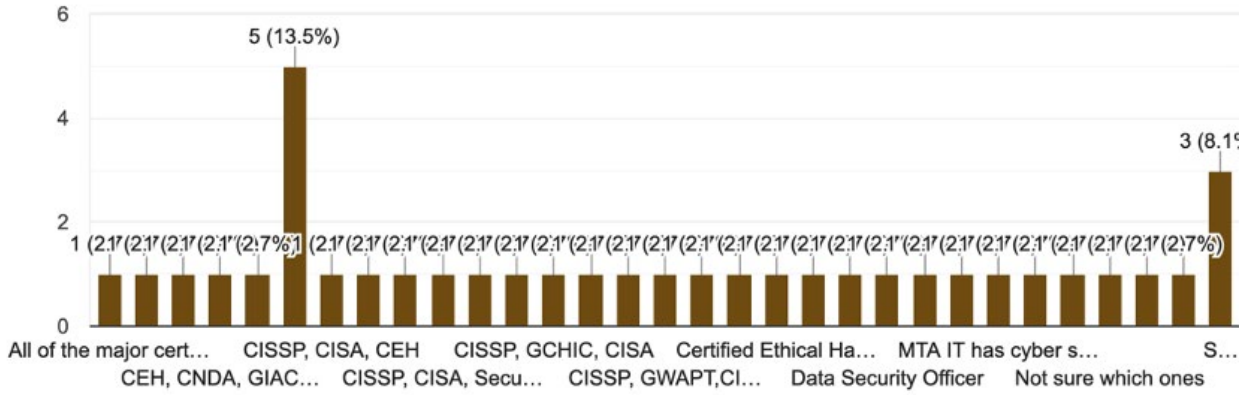
Data from the following survey will be used in aggregate to provide an understanding for both industry and policy leaders as to the current state of cybersecurity preparedness in surface transit. Any information or views that you provide will be treated confidentially with no attribution to you or your employer without your express approval.



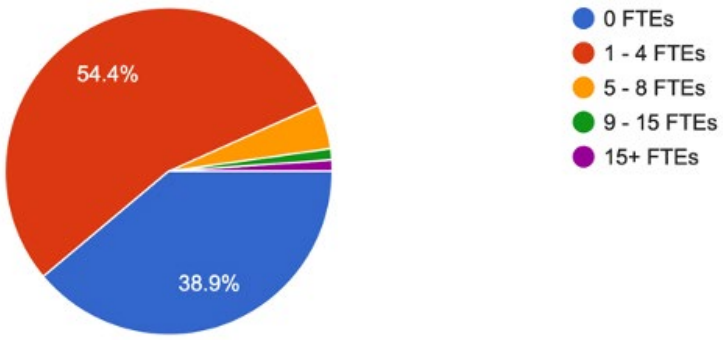
Do you or one of your staff have one or more cybersecurity related certifications?
90 responses



If yes, what are they?
37 responses

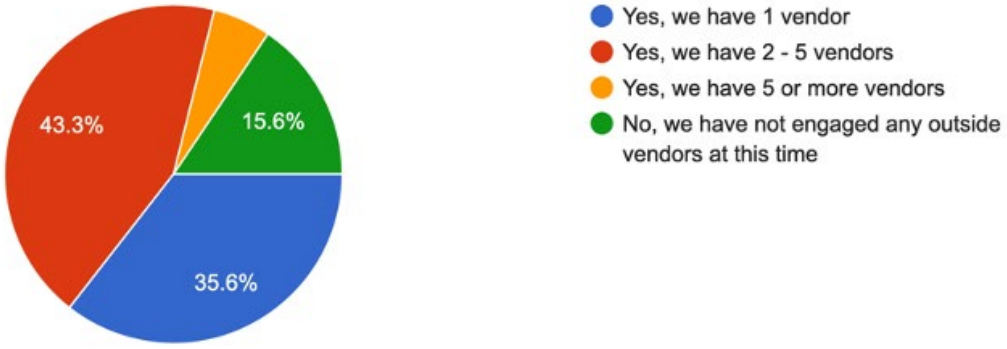


What is your internal headcount dedicated to cybersecurity preparedness? (in full time equivalents (FTE), meaning if you have two people that spend ...rsecurity preparedness, that would equal one FTE)
90 responses



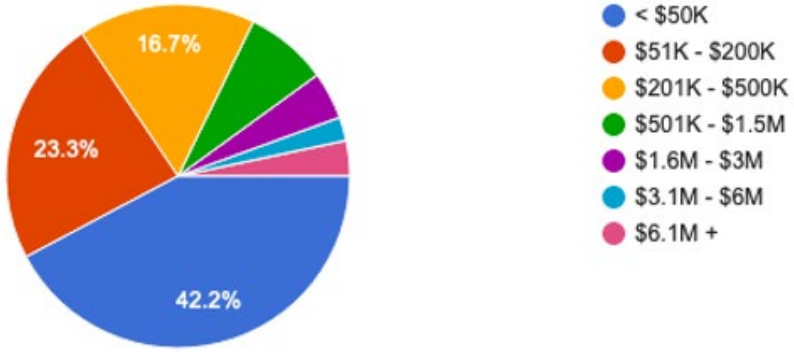
Have you engaged outside vendors to provide tools, software and support to assist with cybersecurity preparedness?

90 responses



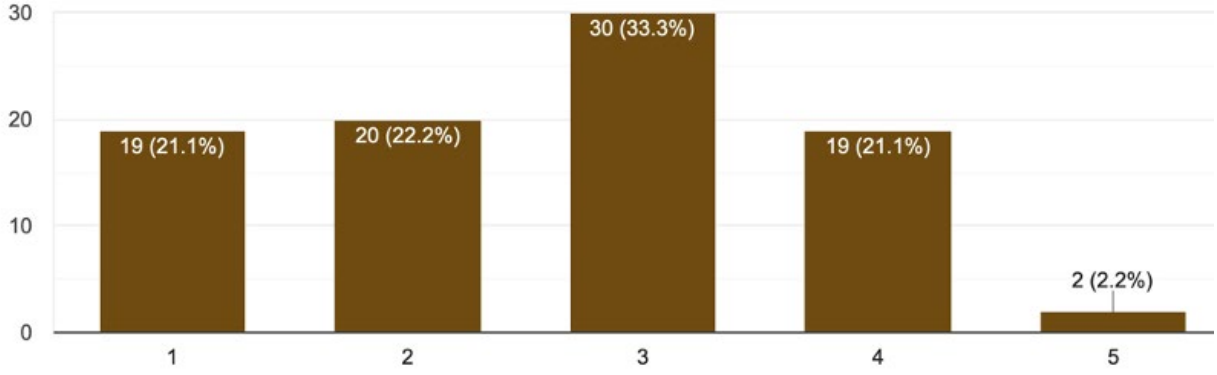
What is your budget for cybersecurity preparedness, including both internal staff and outside vendor support?

90 responses



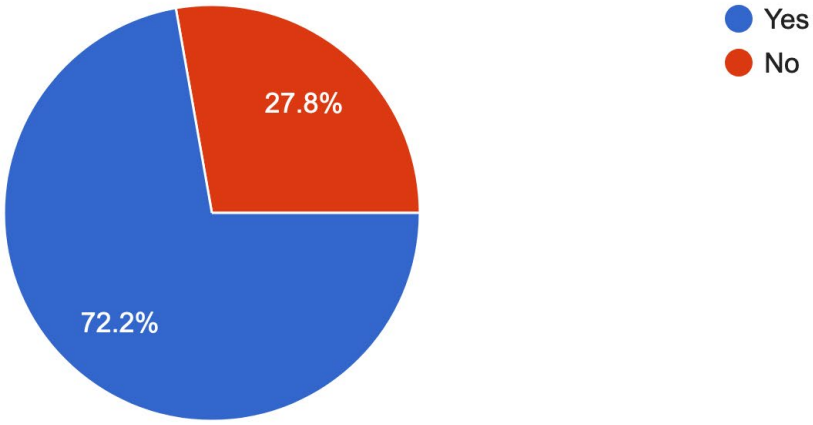
Do you have the resources (e.g., funding, training, other support) you need for cybersecurity preparedness?

90 responses



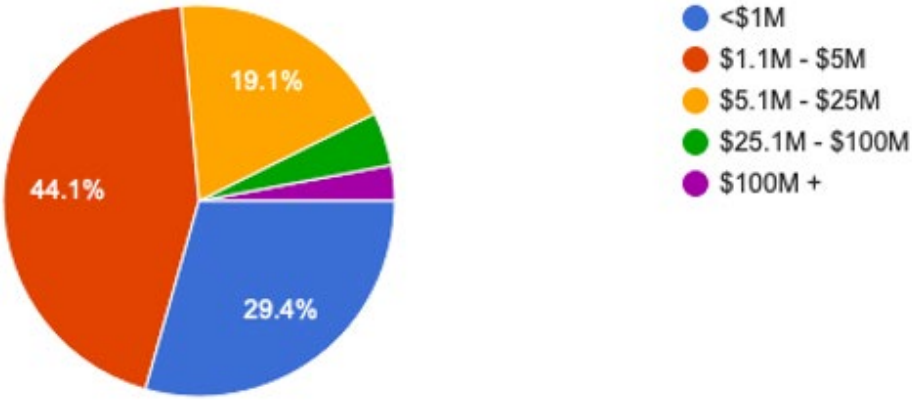
Do you have cybersecurity insurance?

90 responses



If so, what is your approximate coverage limit?

68 responses

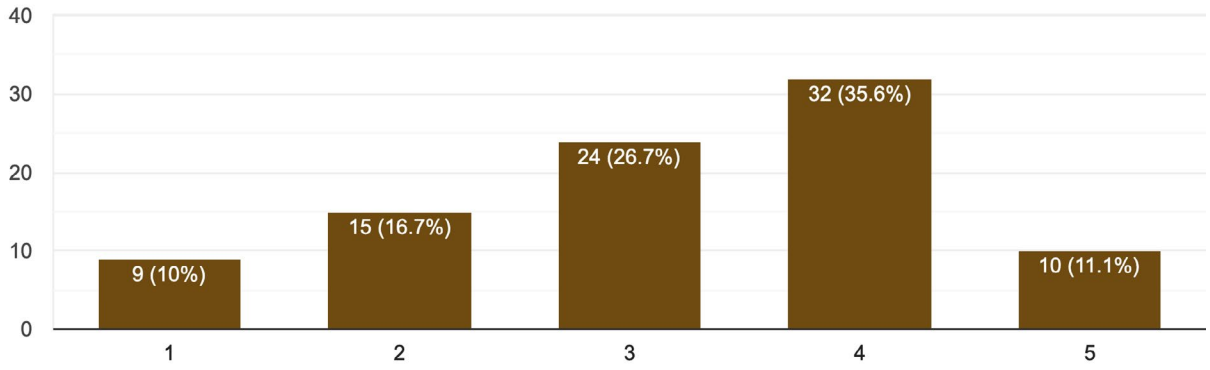


Do you process and/or store customer payment information (e.g., data related to credit cards, bank accounts) directly?

90 responses

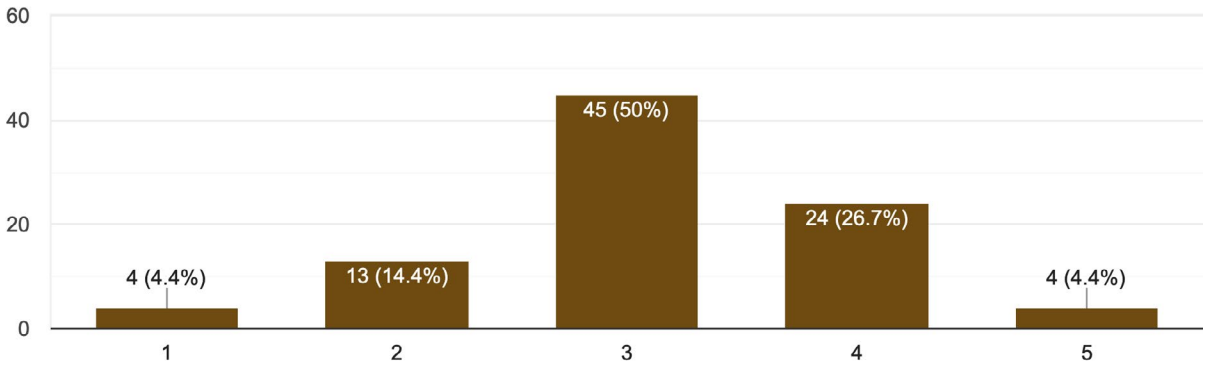
Do you have access to information and guidance that helps you implement your cybersecurity preparedness program?

90 responses

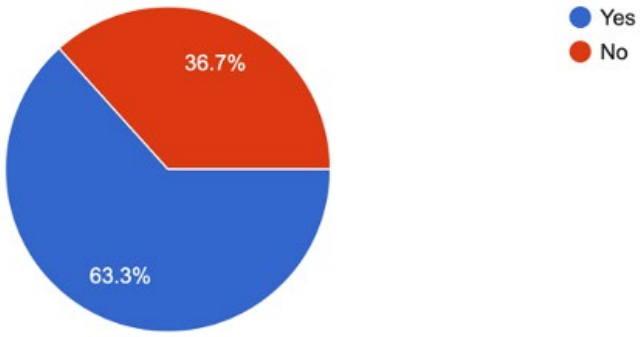


How prepared would you say your organization is in managing and defending against cybersecurity threats?

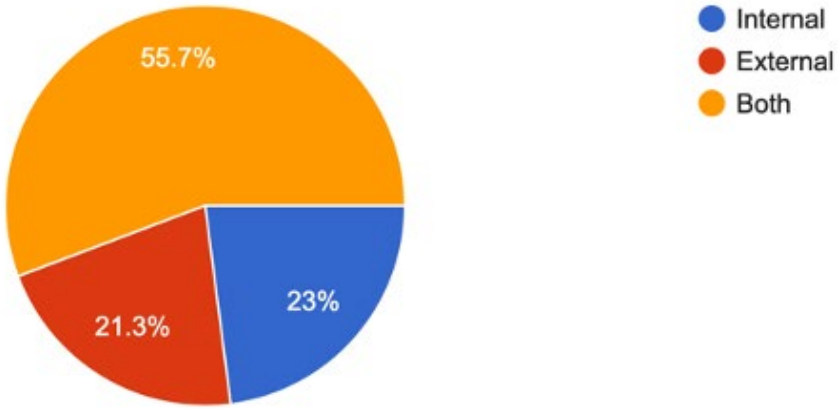
90 responses



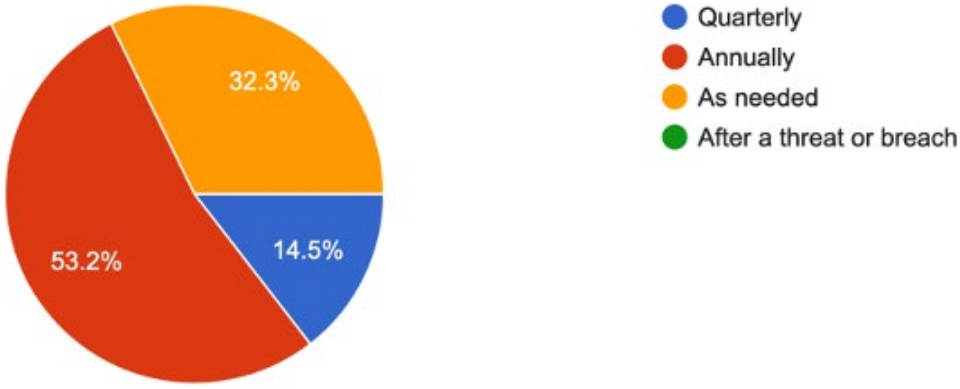
Is there a process (either internal or external to your organization) that audits your cybersecurity preparedness program or establishes some other accountability mechanism for that program?
90 responses



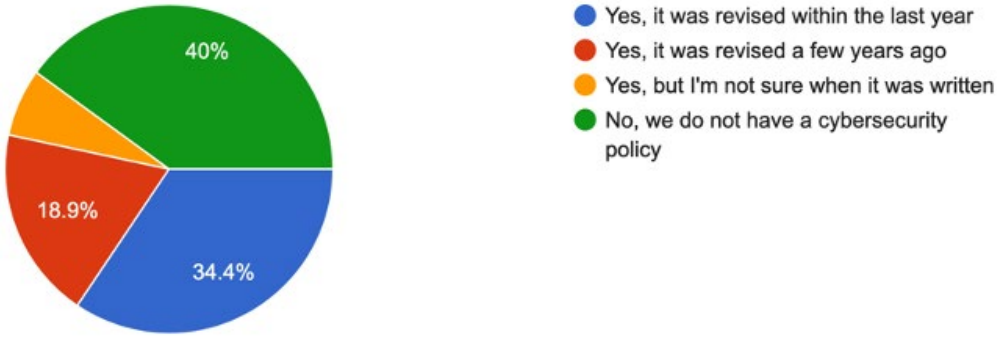
If yes, is the process internal or external?
61 responses



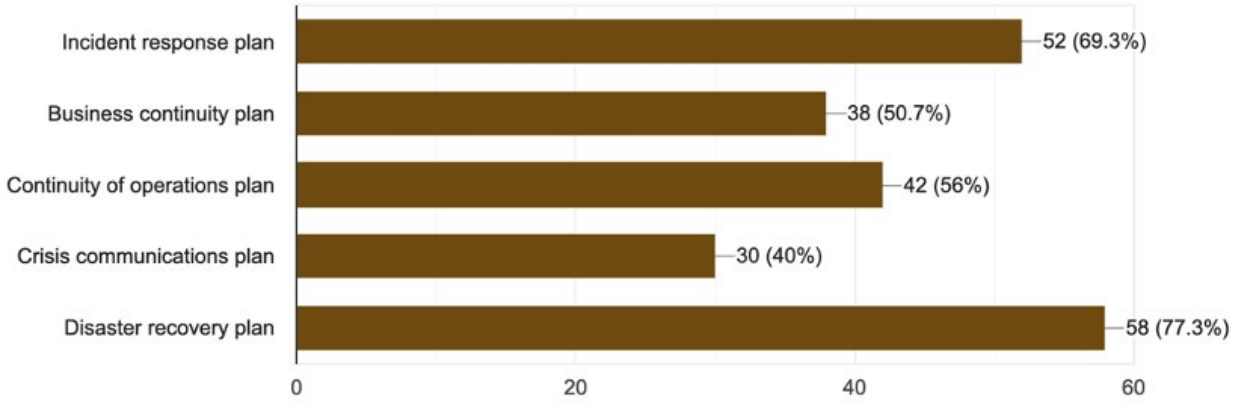
If yes, how frequent is the audit?
62 responses



Do you have a documented cybersecurity policy? If so, how often is it revised?
90 responses



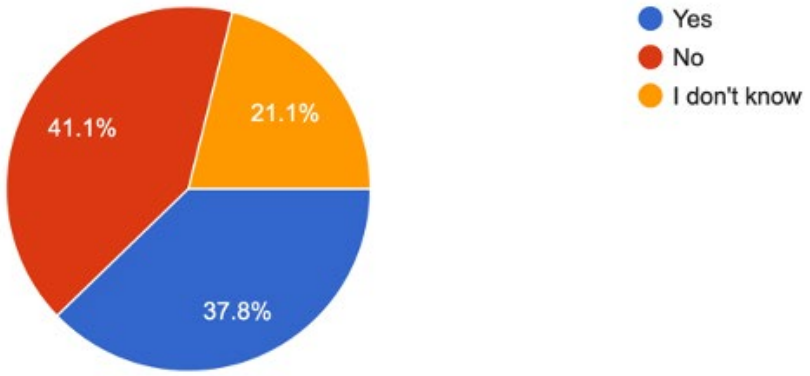
Do you have a (check all that apply):
75 responses



Do you have a documented incident response plan? If so, when was your last drill?
90 responses

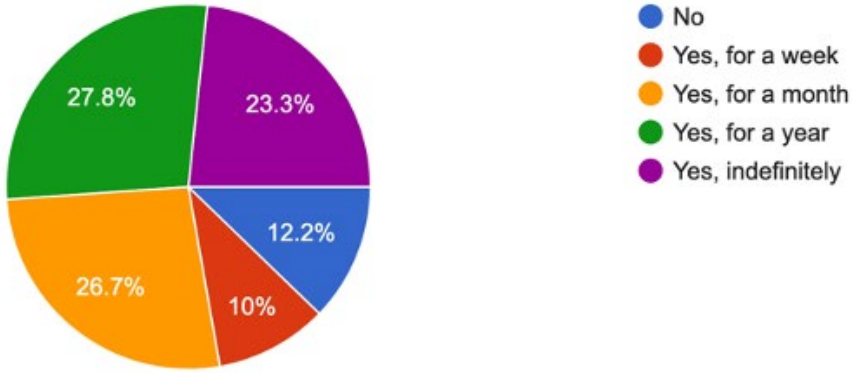
Do you have standard clauses in your vendor contracts related to cybersecurity?

90 responses



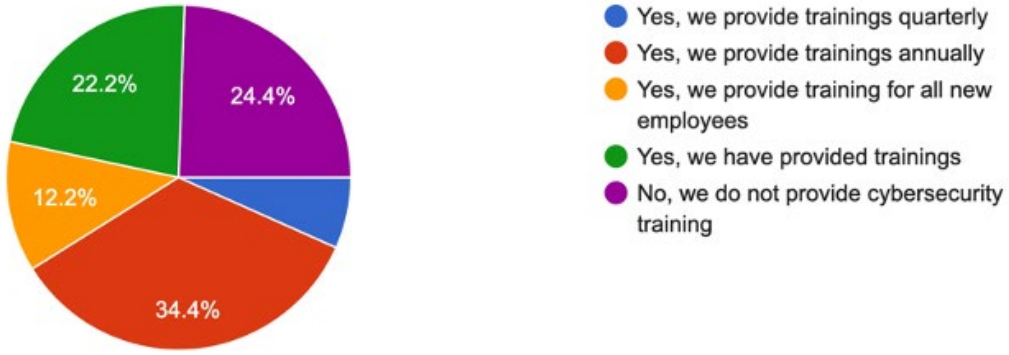
Do you retain logs on your network? If so, for how long?

90 responses

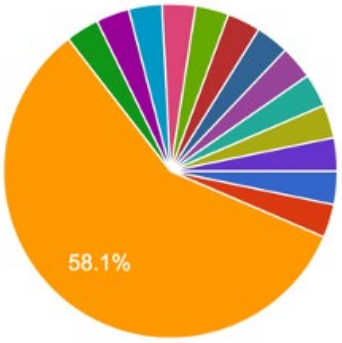


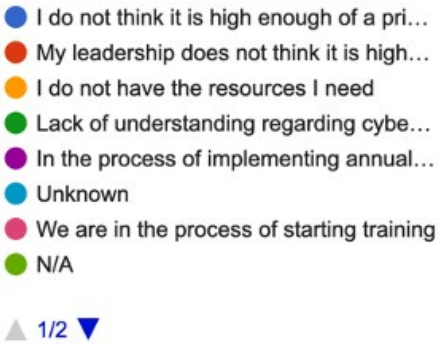
Do you have regular cybersecurity training? How often? Who is trained?

90 responses



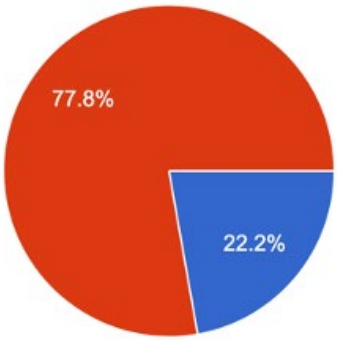
If no, is there a particular reason you are not providing cybersecurity training?
31 responses





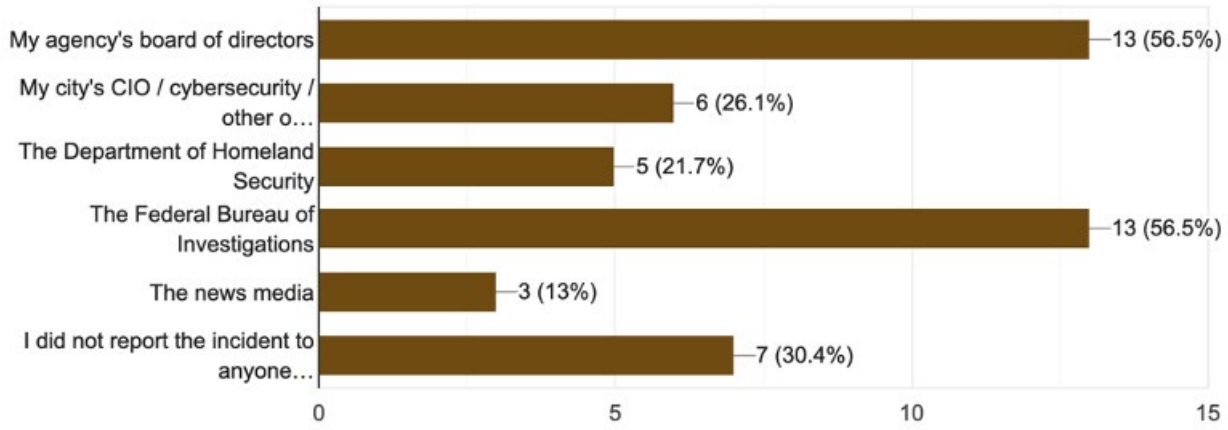
- Unknown
- It was not a priority until recently.
- Small Staff - starting to get more into security.
- Wouldn't know where to start.
- Lack of understanding regarding cybersecurity. Requesting funds FY21

Have you had an incident? An incident is described as a cybersecurity event where an intrusion was made into your systems, and a material loss or ...tions systems were offline for greater than 1 hour.
90 responses



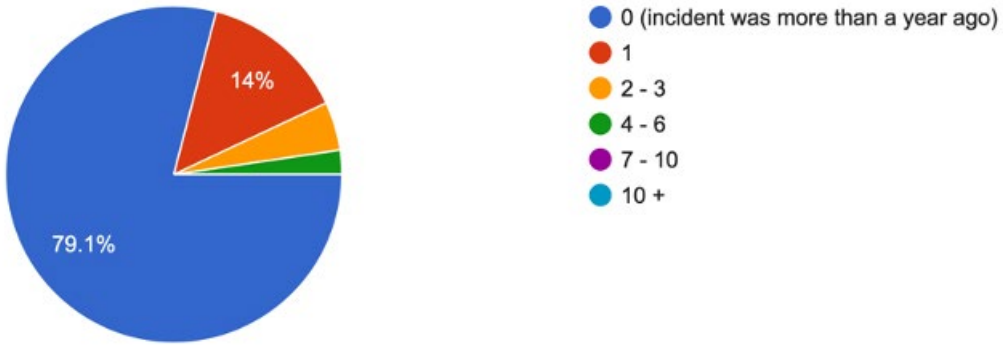
If yes, to whom did you report the incident?

23 responses



If yes, how many in the past year?

43 responses



ABBREVIATIONS AND ACRONYMS

AASHTO	American Association of State Highway Transportation Officials
ABA	American Bus Association
AG	Attorney General
AI	Artificial Intelligence
API	Application Program Interface
APTA	American Public Transit Association
BASE	Baseline Assessment and Security Enhancement
BART	Bay Area Transit Authority
BEC	Business Email Compromise
BRT	Bus Rapid Transit
CDOT	Colorado Department of Transportation
CIO	Chief Information Officer
C-IST	Cyber Infrastructure Survey Tool
CISA	Cybersecurity and Infrastructure Agency
CRR	Cyber Resilience Review
CSA	Cybersecurity Advisors
DOD	United States Department of Defense
DOT	United States Department of Transportation
DSS	Decision Support System
DHS	United States Department of Homeland Security
DSRC	Dedicated Short-Range Communication
EDM	External Dependency Management
EO	Executive Order
EDA	External Demand Management Assessment
FAQs	Frequently Asked Questions
FBI	Federal Bureau of Investigation
FDIC	Federal Deposit Insurance Corporation
FEMA	Federal Emergency Management Agency
FFIEC	Federal Financial Institutions Examination Council
FHWA	Federal Highway Administration
FTA	Federal Transit Administration
FTC	Federal Trade Commission
FTE	Full Time Equivalent

GPS	Global Positioning Systems
ICT	Information and Communication Technology
ITS America	Intelligent Transportation Society of America
ITS JPO	Intelligent Transportation System Joint Program Office
MaaS	Mobility as a Service
MiC3	Michigan Civilian Cyber Corps
MOD	Mobility on Demand
MTAP	Multi-State Transit Technology Assistance Program
NHTSA	National Highway Traffic Safety Administration
NIST	National Institute of Standards and Technology
NTD	National Transit Database
OSTP	White House Office of Science and Technology Policy
PCI	Payment Card Industry
PCI DSS	Payment Card Industry Data Security Standard
PII	Personally Identifiable Information
PPD	Presidential Policy Directive
PT-ISAC	Public Transportation Information Sharing and Analysis Center
SCADA	Supervisory Control and Data Acquisition
SSA	Sector Specific Agencies
STSI	Surface Transportation Security Inspector
SVBX	Silicon Valley Berryessa Extension
TNC	Transportation Network Company
TSA	Transportation Security Agency
TSS	Transportation Systems Sector
UITP	International Association of Public Transport
US-CERT	United States Computer Emergency Readiness Team
USDOT	United States Department of Transportation
WMATA	Washington Metropolitan Area Transit Authority

ENDNOTES

1. Federal Transit Administration (FTA), "National Transit Database (NTD)," last updated April 6, 2020, https://www.transit.dot.gov/ntd/ntd-data (accessed February 12, 2020).

2. Author interview, May 17, 2020.

3. American Public Transportation Association (APTA), 2020 Public Transportation Fact Book, March 2020, 10, https://www.apta.com/wp-content/uploads/APTA-2020-Fact-Book.pdf (accessed March 30, 2020).

4. APTA, 2020 Public Transportation Fact Book, March 2020, 7, https://www.apta.com/wp-content/uploads/APTA-2020-Fact-Book.pdf, (accessed March 30, 2020).

5. Federal Transit Administration (FTA), 2018 National Transit Summaries and Trends, December 2019, 1, https://cms7.fta.dot.gov/sites/fta.dot.gov/files/docs/ntd/data-product/134401/2018-ntst_1.pdf (accessed January 20, 2020).

6. APTA, 2020 Public Transportation Fact Book, March 2020, 7, https://www.apta.com/wp-content/uploads/APTA-2020-Fact-Book.pdf (accessed March 30, 2020).

7. Unlinked passenger trips are an industry measure of ridership and account for each time a passenger boards a transit vehicle, including transfers.

8. APTA, 2020 Public Transportation Fact Book, March 2020, 10, https://www.apta.com/wp-content/uploads/APTA-2020-Fact-Book.pdf (accessed March 30, 2020).

9. APTA, 2020 Public Transportation Fact Book, March 2020, 13, https://www.apta.com/wp-content/uploads/APTA-2020-Fact-Book.pdf (accessed March 30, 2020).

10. APTA, Recommended Practice Securing Control and Communications Systems in Transit Environments Part 1, July 30, 2010, https://www.apta.com/wp-content/uploads/Standards_Documents/APTA-SS-CCS-RP-001-10.pdf (accessed December 19, 2019).

11. Alex Roman, "Q&A with APTA Chair and JTA CEO Nathaniel P. Ford Sr.," *METRO*, February 12, 2018, https://www.metro-magazine.com/mobility/article/728416/q-a-with-apta-chair-and-jta-ceo-nathaniel-p-ford-sr (accessed February 28, 2020).

12. Chris Andrichak et al., "Ensuring Cyber Security for Public Transit Agencies in the Age of Autonomy" (paper presented at APTAtech Transportation Technology Conference, American Public Transportation Association (APTA) Leadership Class of 2019, Columbus, OH, September 2019).

13. APTA, *Cybersecurity Fundamentals for Executives* (video), November 21, 2019, https://www.apta.com/research-technical-resources/aptau/learning-and-development/apta-elearning-courses/ (accessed December 19, 2020).

14. Alex Roman, "Q&A with APTA Chair and JTA CEO Nathaniel P. Ford Sr.," *METRO*, February 12, 2018, https://www.metro-magazine.com/mobility/article/728416/q-a-with-apta-chair-and-jta-ceo-nathaniel-p-ford-sr (accessed February 28, 2020).

15. Caroline Cournoyer, "Hackers Attack Transit System in California's Capital," *Governing*, November 22, 2017, https://www.governing.com/topics/transportation-infrastructure/tns-sacramento-transit-bitcoin-hacker.html (accessed January 24, 2020).

16. Andy Greenberg, "Hackers Hijack a Big Rig Truck's Accelerator and Brakes," *Wired*, August 2, 2016, https://www.wired.com/2016/08/researchers-hack-big-rig-truck-hijack-accelerator-brakes/ (accessed January 24, 2020).

17. Ed Merlis was a researcher who withdrew from this study due to illness.

18. The 287 U.S.-based public transit operators included in this report represent approximately 13% of the total number of public transit operators in the United States, according to NTD data.

19. APTA, "About APTA," November 22, 2019, https://www.apta.com/about (accessed May 15, 2020).

20. Todd Litman, "Public Transportation's Impact on Rural and Small Towns," American Public Transportation Association, https://www.apta.com/wp-content/uploads/Resources/resources/reportsandpublications/Documents/APTA-Rural-Transit-2017.pdf (accessed May 15, 2010).

21. APTA, 2020 Public Transportation Fact Book, 10, March 2020 https://www.apta.com/wp-content/uploads/APTA-2020-Fact-Book.pdf (accessed March 30, 2020).

22. 2019 NTD Data, Author Analysis.

23. This grouping by operating expenses is a common informal breakdown used within the industry and was provided by a Senior Policy Analyst at APTA.

24. 2019 NTD Data, Author Analysis.

25. These are the "Five Functions" that act as the backbone for the Cybersecurity Framework established by the National Institute of Standards and Technology (originally established in February 2014). https://www.nist.gov/cyberframework/online-learning/five-functions (accessed February 28, 2020).

26. APTA, 2020 Public Transportation Fact Book, 16, March 2020, https://www.apta.com/wp-content/uploads/APTA-2020-Fact-Book.pdf (accessed March 30, 2020).

27. Author interview, May 5, 2020.

28. APTA, 2019 Fare Database, 2019, 185-186, https://www.apta.com/research-technical-

resources/transit-statistics/fare-database/ (accessed February 12, 2020).

29. For more details about new mobility initiatives, see the APTA Mobility Innovation Hub: https://www.apta.com/research-technical-resources/mobility-innovation-hub/.

30. Alicja Grzadkowska, "Transportation is now the third most vulnerable sector exposed to cyber attacks," *Insurance Business*, July 24, 2018, https://www.insurancebusinessmag.com/us/news/cyber/transportation-is-now-the-third-most-vulnerable-sector-exposed-to-cyberattacks-106900.aspx (accessed January 24, 2020).

31. Of the 70 agencies that responded "No" to having an incident, several answered follow-up questions intended only for those that had experienced an incident. The researchers surmise that this was unclear and took their response to the initial question at face value. The first question read, "If yes, to whom did you report the incident?" Four agencies that responded "No" to the first question answered this one. The second follow-up question was, "If yes, how many in the past year?" and 24 of the 70 agencies responded with "0" to this question.

32. Dell Technologies,. "Global Data Protection Index: Cloud Environments," March 2020, 2, 5, https://www.delltechnologies.com/en-us/data-protection/gdpi/index.htm#overlay=//www.dellemc.com/en-us/collaterals/unauth/presentations/products/data-protection/dell-gdpi-2019-key-findings-deck-dell-branding.pdf (accessed May 15, 2020).

33. Raymond Pompon et al., "2018 Phishing and Fraud Reports: Attacks Peak During the Holidays," F5 Labs, November 8, 2018, https://www.f5.com/labs/articles/threat-intelligence/2018-phishing-and-fraud-report--attacks-peak-during-the-holidays (accessed January 24, 2020).

34. Chris Andrichak et al., "Ensuring Cyber Security for Public Transit Agencies in the Age of Autonomy" (paper presented at APTAtech Transportation Technology Conference, APTA Leadership Class of 2019, Columbus, OH, September 2019).

35. Federal Bureau of Investigation, Public Service Announcement, Alert # I-071218-PSA, "Business Email Compromise the 12 Billion Dollar Scam," July 12, 2019, https://www.ic3.gov/media/2018/180712.aspx (accessed January 21, 2020).

36. IBM. "Cost of a Data Breach Report 2019." p. 3. (accessed May 15, 2020) https://www.ibm.com/downloads/cas/ZBZLY7KL?_ga=2.117789001.175494517.1589983307-671013754.1589308482

37. Michael Beckerman, "Americans Will Pay a Price for State Privacy Laws," *The New York Times*, October 14, 2019, https://www.nytimes.com/2019/10/14/opinion/state-privacy-laws.html (accessed February 24, 2019).

38. BakerHostetler, Building Cyber Resilience, 2018, 10, https://f.datasrvr.com/fr1/518/85193/2018_BakerHostetler_Data_Security_Incident_Response_Report.pdf

(accessed February 24, 2020).

39. PCI Security Standards Council®, "PCI Security" https://www.pcisecuritystandards.org/pci_security/ (accessed May 20, 2020).

40. Alicja Grzadkowska, "Transportation is now the third most vulnerable sector exposed to cyber attacks," *Insurance Business*, July 24, 2018, https://www.insurancebusinessmag.com/us/news/cyber/transportation-is-now-the-third-most-vulnerable-sector-exposed-to-cyberattacks-106900.aspx (accessed January 24, 2020).

41. Alicja Grzadkowska, "Transportation is now the third most vulnerable sector exposed to cyber attacks," *Insurance Business*, July 24, 2018, https://www.insurancebusinessmag.com/us/news/cyber/transportation-is-now-the-third-most-vulnerable-sector-exposed-to-cyberattacks-106900.aspx (accessed January 24, 2020).

42. Stan Engelbrecht, "Why Mass Transit Could Be the Next Big Target for Cyber Attacks-and What to Do About It," *Security Week*, April 13, 2018, https://www.securityweek.com/why-mass-transit-could-be-next-big-target-cyber-attacks—and-what-do-about-it (accessed March 13, 2020).

43. James R. Slaby, "Ransomware Still Threatens the Transportation and Logistics Industry," Acronis, https://www.acronis.com/en-us/articles/ransomware-logistics/ (accessed January 20, 2020).

44. Tamara Chuang, "How SamSam ransomware took down CDOT and how the state fought back -- twice," *The Colorado Sun*, February 3, 2020, https://coloradosun.com/2020/02/03/how-samsam-ransomware-took-down-cdot-and-how-the-state-fought-back-twice/ (accessed February 19, 2020).

45. Tamara Chuang, "How SamSam ransomware took down CDOT and how the state fought back -- twice," *The Colorado Sun*, February 3, 2020, https://coloradosun.com/2020/02/03/how-samsam-ransomware-took-down-cdot-and-how-the-state-fought-back-twice/ (accessed February 19, 2020).

46. Lee Matthews, "NotPetya Ransomware Attack Costs Shipping Giant Maersk Over $200 Million," *Forbes*, August 16, 2017, https://www.forbes.com/sites/leemathews/2017/08/16/notpetya-ransomware-attack-cost-shipping-giant-maersk-over-200-million/#2b9eac584f9a (accessed February 19, 2020).

47. Brian Krebs, "Target Hackers Broke in Via HVAC Company," Krebs on Security. February 2014, https://krebsonsecurity.com/2014/02/target-hackers-broke-in-via-hvac-company/ (accessed February 19, 2020).

48. United States Senate, Committee on Armed Services, Inquiry into Counterfeit Electronic Parts in the Department of Defense Supply Chain, 112 Congress, 2nd Session, Report 112-167, May 21, 2012, https://www.armed-services.senate.gov/imo/media/doc/Counterfeit-Electronic-Parts.pdf (accessed May 15, 2020).

49. United States Senate, Committee on Armed Services, Inquiry into Counterfeit Electronic Parts in the Department of Defense Supply Chain, 112 Congress, 2nd Session, Report 112-167, i, May 21, 2012, https://www.armed-services.senate.gov/imo/media/doc/Counterfeit-Electronic-Parts.pdf (accessed April 7, 2020).

50. "Record Number of IPR Seizures in FY17 for CBP, ICE," U.S. Customs and Border Protection, March 5, 2018, https://www.cbp.gov/newsroom/national-media-release/record-number-ipr-seizures-fy17-cbp-ice (accessed May 15, 2020).

51. Donald J. Trump, Executive Order 13873 (2019), Securing the Information and Communications Technology and Services Supply Chain, *84 FR 22689*, https://www.federalregister.gov/documents/2019/05/17/2019-10538/securing-the-information-and-communications-technology-and-services-supply-chain.

52. United State Senate. S.1760 National Defense Authorization Act for Fiscal Year 2020, Section 7613, 116th Congress, https://www.congress.gov/bill/116th-congress/senate-bill/1790/text (accessed April 7, 2020).

53. Kyle Malo, WMATA's Supply Chain Cybersecurity Program, Email, May 21, 2020.

54. Donald J. Trump, Executive Order-13800 Strengthening the Cybersecurity of Federal Networks and Critical Infrastructure, *82 FR 22391*, May 16, 2017.

55. Cybersecurity and Infrastructure Security Agency (CISA), "Critical Infrastructure Sectors," https://www.dhs.gov/cisa/critical-infrastructure-sectors (accessed March 13, 2020).

56. Barack Obama, Presidential Policy Directive-21, Washington, D.C.: The White House, February 12, 2013.

57. Barack Obama. Executive Order 13636, Improving Critical Infrastructure Cybersecurity, 78 FR 11737, February 19, 2013, https://www.federalregister.gov/documents/2013/02/19/2013-03915/improving-critical-infrastructure-cybersecurity.

58. National Institute of Standards and Technology (NIST), "Framework for Improving Critical Infrastructure Cybersecurity," February 2014, https://tsapps.nist.gov/publication/get_pdf.cfm?pub_id=915476 (accessed December 19, 2019).

59. CISA, "ABOUT CISA," https://www.cisa.gov/about-cisa (accessed March 13, 2020).

60. Transportation Security Administration (TSA), "Mission," https://www.tsa.gov/about/tsa-mission (accessed March 13, 2020).

61. TSA, "TSA Releases Cybersecurity Roadmap," December 4, 2018, https://www.tsa.gov/news/releases/2018/12/04/tsa-releases-cybersecurity-roadmap (accessed March 13, 2020).

62. TSA, "Cybersecurity Roadmap 2018," 4 November 2018, https://www.tsa.gov/sites/default/files/documents/tsa_cybersecurity_roadmap.pdf (accessed March 13, 2020).

63. Department of Homeland Security (DHS), Transportation Systems Sector Cybersecurity Framework Implementation Guidance, 2 June 26, 2015, https://www.cisa.gov/sites/default/files/publications/tss-cybersecurity-framework-implementation-guide-2016-508v2_0.pdf (accessed February 24, 2020).

64. DHS, Transportation Systems Sector Cybersecurity Framework Implementation Guidance, June 26, 2015, 3, https://www.cisa.gov/sites/default/files/publications/tss-cybersecurity-framework-implementation-guide-2016-508v2_0.pdf (accessed February 24, 2020).

65. CISA, "Transportation Systems Sector," https://www.cisa.gov/transportation-systems-sector (accessed March 13, 2020).

66. National Institute of Standards and Technology (NIST), "Cybersecurity Framework," updated May 21, 2020, http://www.nist.gov/cyberframework/ (accessed May 22, 2020).

67. CISA, Transportation Systems Sector Cybersecurity Framework Implementation Guide, June 26, 2015, https://www.cisa.gov/publication/tss-cybersecurity-framework-implementation-guide (accessed March 13, 2020).

68. DHS, "Cybersecurity Advisor," 2017, https://www.bu.edu/tech/files/2017/09/DHS_CSA_Fact_Sheet_2017-1.pdf (accessed March 13, 2020).

69. DHS, "Cybersecurity Advisor," 2017, https://www.bu.edu/tech/files/2017/09/DHS_CSA_Fact_Sheet_2017-1.pdf (accessed March 13, 2020).

70. Federal Transit Administration (FTA), The Public Transportation System Security and Emergency Preparedness Planning Guide, January 2003, https://www.transit.dot.gov/sites/fta.dot.gov/files/docs/PlanningGuide.pdf (accessed March 13, 2020).

71. FTA, Security and Emergency Preparedness Action Items for Transit Agencies, September 2014, https://www.transit.dot.gov/sites/fta.dot.gov/files/docs/508_new_top_17.pdf (accessed March 13, 2020).

72. FTA, Security and Emergency Preparedness Action Items for Transit Agencies, September 2014, https://www.transit.dot.gov/sites/fta.dot.gov/files/docs/508_new_top_17.pdf (accessed March 13, 2020).

73. FTA, Security and Emergency Preparedness Action Items for Transit Agencies, September 2014, 8, https://www.transit.dot.gov/sites/fta.dot.gov/files/docs/508_new_top_17.pdf (accessed March 13, 2020).

74. US-CERT is CISA's 24-hour operational arm that is responsible for analyzing and

reducing cyber threats and vulnerabilities, disseminating cyber threat warning information, and coordinating incident response activities.

75. PT-ISAC is the public transportation's 24/7 incident reporting and threat warning entity that establishes the sector's specific information/intelligence requirements for incidents, threats, and vulnerabilities.

76. FTA. Security and Emergency Preparedness Action Items for Transit Agencies. September 2014, 20-21, https://www.transit.dot.gov/sites/fta.dot.gov/files/docs/508_new_top_17.pdf (accessed March 13, 2020).

77. TSA, Security Training for Surface Transportation Employees, *85FR16456*, March 23, 2020, https://www.federalregister.gov/documents/2020/03/23/2020-05126/security-training-for-surface-transportation-employees.

78. FTA, "Frequently Asked Questions: Transit Bus Automation Policy," July 11, 2019, https://www.transit.dot.gov/sites/fta.dot.gov/files/docs/research-innovation/134506/transit-bus-automation-faqs_0.pdf (accessed May 19, 2020).

79. National Highway Traffic Safety Administration (NHTSA), "Technology & Innovation," March 16, 2018, https://www.nhtsa.gov/technology-innovation (accessed May 15, 2020).

80. Federal Highway Administration (FHWA), Federal Highway Administration (FHWA) Cybersecurity Program (CSP) Handbook, December 2017, https://www.fhwa.dot.gov/legsregs/directives/orders/csp_handbook.pdf (accessed January 20, 2020).

81. Department of Transportation (DOT), "Cybersecurity Fact Sheet," https://www.its.dot.gov/factsheets/pdf/cybersecurity_factsheet.pdf (accessed January 20, 2020).

82. DOT, Intelligent Transportation Systems Joint Program Office, Strategic Plan 2020-2025, May 6, 2020, 32, https://www.its.dot.gov/stratplan2020/ITSJPO_StrategicPlan_2020-2025.pdf (accessed May 11, 2020).

83. DOT, "Cybersecurity and Intelligent Transportation Systems: A Best Practices Guide," U.S. DOT FHWA-JPO-19-763, September 17, 2019, https://rosap.ntl.bts.gov/view/dot/42461 (accessed February 24, 2020).

84. Author interview, December 18, 2019.

85. "Michigan Cyber Civilian Corps," SOM – Michigan.gov, https://www.michigan.gov/som/0,4669,7-192-78403_78404_78419---,00.html (accessed May 19, 2020).

86. "MDDF Units," Maryland.gov, https://military.maryland.gov/mddf/Pages/MDDF-Units.aspx (accessed May 19, 2020).

87. Cal Poly California Cybersecurity Institute, "About the CCI," https://cci.calpoly.edu/

about (accessed May 19, 2020).

88. Jim Siegel, "An Ohio Cybersecurity Reserve Could Soon Respond to Network Emergencies," Government Technology, September 18, 2018, http://www.govtech.com/security/An-Ohio-Cybersecurity-Reserve-Could-Soon-Respond-to-Network-Emergencies.html (accessed May 19, 2020).

89. "Bridging State-Level Cybersecurity Resources," Lawfare, October 31, 2019, https://www.lawfareblog.com/bridging-state-level-cybersecurity-resources (accessed May 18, 2020).

90. CISA, "Resources for State, Local, Tribal, and Territorial (SLTT) Governments," https://www.us-cert.gov/resources/sltt#geo (accessed May 18, 2020).

91. In the authors' consideration of organization providing support to the transit industry, the various Information Sharing and Analysis Centers (ISACs) that provide threat data and other critical information to the transportation industry were not included. They include the Surface Transportation ISAC, the Public Transportation ISAC, and the Over-the-Road Bus ISAC. These entities perform an important role in assisting transit agencies to develop their awareness of cyber threats, but the focus in this discussion is on those organizations that assist transit agencies in the actual design and implementation of a cybersecurity preparedness program (in which information from the ISACS inevitably plays a key role).

92. APTA, Recommended Practice Cybersecurity Considerations for Public Transit, October 17, 2014, https://www.apta.com/research-technical-resources/standards/security/apta-ss-ecs-rp-001-14/ (accessed December 19, 2019).

93. APTA, Recommended Practice Securing Control and Communications Systems in Transit Environments Part 1: Elements, Organization and Risk Assessment/Management July 30, 2010, https://www.apta.com/research-technical-resources/standards/security/apta-ss-ccs-rp-001-10/ (accessed December 19, 2019); APTA, Recommended Practice Securing Control and Communications Systems in Rail Transit Environments Part II: Defining a Security Zone Architecture for Rail Transit and Protecting Critical Zones, June 28, 2013, https://www.apta.com/research-technical-resources/standards/security/apta-ss-ccs-rp-002-13/ (accessed December 19, 2019).

94. American Association of State Highway Transportation Officials (AASHTO), "Council on Public Transportation," https://ptc.transportation.org/ (accessed May 15, 2020).

95. AASHTO, "Council on Public Transportation," https://ptc.transportation.org/ (accessed May 15, 2020).

96. FTA, "Triennial Reviews," https://www.transit.dot.gov/funding/grantee-resources/triennial-reviews/triennial-reviews (accessed May 15, 2020).

97. Federal Deposit Insurance Corporation (FDIC), "Cyber Challenge: A Community Bank

Cyber Exercise," https://www.fdic.gov/regulations/resources/director/technical/cyber/cyber.html (accessed March 13, 2020).

98. Countermeasures Assessment & Security Experts, LLC and Western Management and Consulting, LLC, *Security 101: A Physical and Cybersecurity Primer for Transportation Agencies*, pre-publication draft of NCHRP Research Report 930, Transportation Research Board, Washington, D.C., 2009: 100. http://onlinepubs.trb.org/onlinepubs/nchrp/nchrp_rpt_930.pdf.

99. Michael Cobb, "Best practices for audit, log review for IT security investigations," Computer Weekly, August 8, 2011, https://www.computerweekly.com/tip/Best-practices-for-audit-log-review-for-IT-security-investigations (accessed May 15, 2020).

100. Karen Kent and Murugiah Souppaya, Guide to Computer Security Log Management, National Institute of Standards and Technology (NIST), September 2006, https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-92.pdf (accessed May 15, 2020).

101. Countermeasures Assessment & Security Experts, LLC and Western Management and Consulting, LLC, *Security 101: A Physical and Cybersecurity Primer for Transportation Agencies*, pre-publication draft of NCHRP Research Report 930, Transportation Research Board, Washington, D.C., 2009: http://onlinepubs.trb.org/onlinepubs/nchrp/nchrp_rpt_930.pdf.

102. NIST, "Information Security Handbook: A Guide for Managers," October 2006, https://csrc.nist.gov/publications/detail/sp/800-100/final (accessed February 28, 2020).

103. APTA, Recommended Practice Cybersecurity Consideration for Public Transit, October 17, 2014, 12-13, https://www.apta.com/research-technical-resources/standards/security/apta-ss-ecs-rp-001-14/ (accessed December 19, 2019).

104. Author interview, October 31, 2019.

105. ISC^2, "CISSP The World's Premiere Cybersecurity Certification," https://www.isc2.org/Certifications/CISSP (accessed May 15, 2020).

106. "EC Council Certification," EC Council, https://cert.eccouncil.org/ (accessed May 15, 2020).

107. Author interview, 31 October 2019.

108. "10 Statistics that Summarize the State of Cybersecurity in Financial Services," *Security Boulevard*, November 12, 2019, https://securityboulevard.com/2019/11/10-statistics-that-summarize-the-state-of-cybersecurity-in-financial-services/ (accessed May 1, 2020).

109. "Pursuing cybersecurity maturity at financial institutions," Deloitte, May 1, 2019,

https://www2.deloitte.com/us/en/insights/industry/financial-services/cybersecurity-maturity-financial-institutions-cyber-risk.html (accessed May 15, 2020).

110. Of the 90 agencies that responded to the survey, employee data were not available for 22 of them. These agencies were excluded from this analysis. In addition, three agencies with data were excluded, as their employee counts appear very low given their size. This is likely due to the outsourcing of many of their operations.

111. Eleven small agencies were excluded from this metric. Respondents were asked to select a range for their cyber budget. The range for these agencies was too great to make this metric meaningful.

112. NuHarbor Security, "Information Security Staffing Guide," March 15, 2019, https://www.nuharborsecurity.com/information-security-staffing-guide (accessed May 1, 2020).

113. APTA, *Cybersecurity Fundamentals for Executives* (video), November 21, 2019, https://www.apta.com/research-technical-resources/aptau/learning-and-development/apta-elearning-courses/ (accessed December 19, 2020).

BIBLIOGRAPHY

Allen, Julia, Gregory Crabb, Pamela D. Curtis, Brendan Fitzpatrick, Nader Mehravari, and David Tobar. “Structuring the Chief Information Security Officer Organization,” Carnegie Mellon University. October 2015. https://resources.sei.cmu.edu/asset_files/TechnicalNote/2015_004_001_446198.pdf (accessed February 28, 2019).

American Association of State Highway Transportation (AASHTO). “Council on Public Transportation.” https://ptc.transportation.org/ (accessed May 15, 2020).

American Public Transportation Association (APTA). 2020 Public Transportation Fact Book. March 2020. https://www.apta.com/wp-content/uploads/APTA-2020-Fact-Book.pdf (accessed March 30, 2020).

American Public Transportation Association (APTA). Recommended Practice “Enterprise Cybersecurity Training and Awareness.” March 27, 2019. https://www.apta.com/wp-content/uploads/APTA-SS-ECS-RP-002-19.pdf (accessed December 19, 2020).

American Public Transportation Association.(APTA) Recommended Practice Securing Control and Communication Systems in Transit Bus Vehicles and Supporting Infrastructure.” July 7, 2019. https://www.apta.com/research-technical-resources/standards/security/apta-ss-ccs-wp-005-19/ (accessed December 19, 2019).

American Public Transportation Association (APTA). Recommended Practice “Cybersecurity Consideration for Public Transit.” October 17, 2014. https://www.apta.com/research-technical-resources/standards/security/apta-ss-ecs-rp-001-14/ (accessed December 19, 2019).

American Public Transportation Association.(APTA) Recommended Practice “Enterprise Cybersecurity: Involving the Board of Directors and the Executive Suite.” March 27, 2019. https://www.apta.com/research-technical-resources/standards/security/apta-ss-ecs-rp-003-19/ (accessed December 19, 2019).

American Public Transportation Association (APTA). “About APTA.” November 22, 2019. https://www.apta.com/about (accessed May 15, 2020).

American Public Transportation Association (APTA). 2019 Fare Database. 2019. https://www.apta.com/research-technical-resources/transit-statistics/fare-database/ (accessed February 12, 2020).

American Public Transportation Association (APTA). “Mobility Innovation Hub.” https://www.apta.com/research-technical-resources/mobility-innovation-hub/ (accessed May 15, 2020).

American Public Transportation Association (APTA). Cybersecurity Fundamentals for Executives. November 21, 2019. Video. https://www.apta.com/research-technical-

resources/aptau/learning-and-development/apta-elearning-courses/ (accessed December 19, 2020).

American Public Transportation Association (APTA). Recommended Practice "Securing Control and Communications Systems in Transit Environments Part 1: Elements, Organization and Risk Assessment/Management." July 30, 2010. https://www.apta.com/research-technical-resources/standards/security/apta-ss-ccs-rp-001-10/ (accessed December 19, 2019).

American Public Transportation Association (APTA). Recommended Practice "Securing Control and Communications Systems in Rail Transit Environments Part II: Defining a Security Zone Architecture for Rail Transit and Protecting Critical Zones." June 28, 2013. https://www.apta.com/research-technical-resources/standards/security/apta-ss-ccs-rp-002-13/ (accessed December 19, 2019).

Andrichak, Chris, William Benz, Frederick Edwards, Akiko Ito, Donald Luey, Tomika Monterville. "Ensuring Cyber Security for Public Transit Agencies in the Age of Autonomy." Paper presented at the APTAtech Transportation Technology Conference, Columbus, OH, September 2019.

BakerHostetler. Building Cyber Resilience. 2018. https://f.datasrvr.com/fr1/518/85193/2018_BakerHostetler_Data_Security_Incident_Response_Report.pdf (accessed February 24, 2020).

Beckerman, Michael. "Americans Will Pay a Price for State Privacy Laws." *The New York Times*, October 14, 2019. https://www.nytimes.com/2019/10/14/opinion/state-privacy-laws.html (accessed February 24, 2019).

Cal Poly California Cybersecurity Institute. "About the CCI." https://cci.calpoly.edu/about (accessed May 19, 2020).

Chuang, Tamara. "How SamSam ransomware took down CDOT and how the state fought back – twice." *The Colorado Sun*, February 3, 2020. https://coloradosun.com/2020/02/03/how-samsam-ransomware-took-down-cdot-and-how-the-state-fought-back-twice/ (accessed February 19, 2020).

Cobb, Michael. "Best practices for audit, log review for IT security investigations." *Computer Weekly*, August 8, 2011. https://www.computerweekly.com/tip/Best-practices-for-audit-log-review-for-IT-security-investigations (accessed May 15, 2020).

Countermeasures Assessment & Security Experts, LLC and Western Management and Consulting, LLC. *Security 101: A Physical and Cybersecurity Primer for Transportation Agencies.* Pre-publication draft of NCHRP Research Report 930. Washington, D.C.: Transportation Research Board, 2019. http://onlinepubs.trb.org/onlinepubs/nchrp/nchrp_rpt_930.pdf

Cournoyer, Caroline. “Hackers Attack Transit System in California’s Capitol.” Governing. November 22, 2017. https://www.governing.com/topics/transportation-infrastructure/tns-sacramento-transit-bitcoin-hacker.html (accessed January 24, 2020).

Customs and Border Protection, “Record Number of IPR Seizures in FY17 for CBP, ICE.” March 5, 2018. https://www.cbp.gov/newsroom/national-media-release/record-number-ipr-seizures-fy17-cbp-ice (accessed May 15, 2020).

Cybersecurity and Infrastructure Security Agency (CISA). “Critical Infrastructure Sectors.” https://www.dhs.gov/cisa/critical-infrastructure-sectors (accessed March 13, 2020).

Cybersecurity and Infrastructure Security Agency (CISA). “About CISA.” https://www.cisa.gov/about-cisa (accessed March 13, 2020).

Cybersecurity and Infrastructure Security Agency (CISA). “Resources for State, Local, Tribal, and Territorial (SLTT) Governments.” https://www.us-cert.gov/resources/sltt#geo (accessed May 18, 2020).

Cybersecurity and Infrastructure Security Agency (CISA). “Transportation Systems Sector.” https://www.cisa.gov/transportation-systems-sector (accessed March 13, 2020).

Cybersecurity and Infrastructure Security Agency (CISA). Transportation Systems Sector-Specific Plan, 2015. 2015. https://www.cisa.gov/sites/default/files/publications/nipp-ssp-transportation-systems-2015-508.pdf (accessed December 19, 2019)

Cybersecurity and Infrastructure Security Agency (CISA). Transportation Systems Sector Cybersecurity Framework Implementation Guide. June 26, 2015. https://www.cisa.gov/publication/tss-cybersecurity-framework-implementation-guide (accessed March 13, 2020).

Dell Technologies. “Global Data Protection Index: Cloud Environments.” March 2020. https://www.delltechnologies.com/en-us/data-protection/gdpi/index.htm#overlay=//www.dellemc.com/en-us/collaterals/unauth/presentations/products/data-protection/dell-gdpi-2019-key-findings-deck-dell-branding.pdf (accessed May 15, 2020).

Deloitte. “Pursuing cybersecurity maturity at financial institutions.” May 1, 2019. https://www2.deloitte.com/us/en/insights/industry/financial-services/cybersecurity-maturity-financial-institutions-cyber-risk.html (accessed May 15, 2020).

Department of Homeland Security (DHS). “Cybersecurity Advisor.” 2017. https://www.bu.edu/tech/files/2017/09/DHS_CSA_Fact_Sheet_2017-1.pdf (accessed March 13, 2020).

Department of Homeland Security (DHS). Transportation Systems Sector Cybersecurity Framework Implementation Guidance. June 26, 2015. https://www.cisa.gov/sites/default/files/publications/tss-cybersecurity-framework-implementation-guide-2016-508v2_0.pdf (accessed February 24, 2020).

Department of Transportation (DOT). “Cybersecurity Fact Sheet.” https://www.its.dot.gov/factsheets/pdf/cybersecurity_factsheet.pdf (accessed January 20, 2020).

Department of Transportation (DOT). “Cybersecurity and Intelligent Transportation Systems: A Best Practices Guide.” U.S. DOT, FHWA-JPO-19-763. September 17, 2019. https://rosap.ntl.bts.gov/view/dot/42461 (accessed February 24, 2020).

Department of Transportation (DOT). Intelligent Transportation Systems Joint Program Office, Strategic Plan 2020-2025. May 6, 2020. https://www.its.dot.gov/stratplan2020/ITSJPO_StrategicPlan_2020-2025.pdf (accessed May 11, 2020).

EC Council. “EC Council Certification.” https://cert.eccouncil.org/ (accessed May 15, 2020).

Engelbrecht, Stan. “Why Mass Transit Could Be the Next Big Target for Cyber Attacks-and What to Do About It.” *Security Week*, April 13, 2018. https://www.securityweek.com/why-mass-transit-could-be-next-big-target-cyber-attacks—and-what-do-about-it (accessed March 13, 2020).

Federal Bureau of Investigation (FBI). Public Service Announcement, Alert # I-071218-PSA. “Business Email Compromise the 12 Billion Dollar Scam.” July 12, 2019. https://www.ic3.gov/media/2018/180712.aspx (accessed January 21, 2020).

Federal Deposit Insurance Corporation (FDIC). “Cyber Challenge: A Community Bank Cyber Exercise.” https://www.fdic.gov/regulations/resources/director/technical/cyber/cyber.html (accessed March 13, 2020).

Federal Highway Administration (FHWA). Federal Highway Administration (FHWA) Cybersecurity Program (CSP) Handbook. December 2017. https://www.fhwa.dot.gov/legsregs/directives/orders/csp_handbook.pdf (accessed January 20, 2020).

Federal Highway Administration (FHWA). Cybersecurity and Intelligent Transportation Systems, A Best Practice Guide, September 17, 2019, FHWA-JPO-19-763. https://rosap.ntl.bts.gov/view/dot/42461 (accessed January 20, 2020).

Federal Transit Administration (FTA). “Triennial Reviews.” https://www.transit.dot.gov/funding/grantee-resources/triennial-reviews/triennial-reviews (accessed May 15, 2020).

Federal Transit Administration (FTA). National Transit Database (NTD). Last updated April 6, 2020. https://www.transit.dot.gov/ntd/ntd-data (accessed February 12, 2020).

Federal Transit Administration (FTA). 2018 National Transit Summaries and Trends. December 2019. https://cms7.fta.dot.gov/sites/fta.dot.gov/files/docs/ntd/data-product/134401/2018-ntst_1.pdf (accessed January 20, 2020).

Federal Transit Administration (FTA). The Public Transportation System Security and Emergency Preparedness Planning Guide. January 2003. https://www.transit.dot.gov/sites/fta.dot.gov/files/docs/PlanningGuide.pdf (accessed March 13, 2020).

Federal Transit Administration (FTA). Security and Emergency Preparedness Action Items for Transit Agencies. September 2014. https://www.transit.dot.gov/sites/fta.dot.gov/files/docs/508_new_top_17.pdf (accessed March 13, 2020).

Federal Transit Administration (FTA). Frequently Asked Questions: Transit Bus Automation Policy. July 11, 2019. https://www.transit.dot.gov/sites/fta.dot.gov/files/docs/research-innovation/134506/transit-bus-automation-faqs_0.pdf (accessed May 19, 2020).

Federal Financial Institutions Examination Council (FFEIC). "FFEIC Cybersecurity Assessment Tool." May 2017. https://www.ffiec.gov/pdf/cybersecurity/FFIEC_CAT_May_2017.pdf (accessed February 28, 2020).

Friedman, Sam, Nikhil Gokhale. "Pursuing Cybersecurity Maturity at Financial Institutions." Deloitte. May 1, 2019. www2.deloitte.com/us/en/insights/industry/financial-services/cybersecurity-maturity-financial-institutions-cyber-risk.html (accessed February 28, 2020).

Greenberg, Andy. "Hackers Hijack a Big Rig Truck's Accelerator and Brakes." *Wired*, August 2, 2016. https://www.wired.com/2016/08/researchers-hack-big-rig-truck-hijack-accelerator-brakes/ (accessed January 24, 2020).

Grzadkowska, Alicja. "Transportation is now the third most vulnerable sector exposed to cyber attacks." *Insurance Business*, July 24, 2018. https://www.insurancebusinessmag.com/us/news/cyber/transportation-is-now-the-third-most-vulnerable-sector-exposed-to-cyberattacks-106900.aspx (accessed January 24, 2020).

IBM. "Cost of a Data Breach Report 2019." https://www.ibm.com/downloads/cas/ZBZLY7KL?_ga=2.117789001.175494517.1589983307-671013754.1589308482 (accessed May 15, 2020).

ISC². "CISSP The World's Premiere Cybersecurity Certification." https://www.isc2.org/Certifications/CISSP (accessed May 15, 2020).

Kent, Karen, Murugiah Souppaya. Guide to Computer Security Log Management. National Institute of Standards and Technology. September 2006. https://nvlpubs.nist.gov/n istpubs/Legacy/SP/nistspecialpublication800-92.pdf (accessed May 15, 2020).

Krebs, Brian. “Target Hackers Broke in Via HVAC Company.” Krebs on Security. February 2014. https://krebsonsecurity.com/2014/02/target-hackers-broke-in-via-hvac-company/ (accessed February 19, 2020).

Lawfare. “Bridging State-Level Cybersecurity Resources.” October 31, 2019. https://www.lawfareblog.com/bridging-state-level-cybersecurity-resources (accessed May 18, 2020).

Litman, Todd. “Public Transportation’s Impact on Rural and Small Towns.” American Public Transportation Association. https://www.apta.com/wp-content/uploads/Resources/resources/reportsandpublications/Documents/APTA-Rural-Transit-2017.pdf (accessed May 15, 2010).

Maryland.gov. “MDDF Units.” https://military.maryland.gov/mddf/Pages/MDDF-Units.aspx (accessed May 19, 2020).

Matthews, Lee. “NotPetya Ransomware Attack Costs Shipping Giant Maersk Over $200 Million.” *Forbes*, August 16, 2017. https://www.forbes.com/sites/leemathews/2017/08/16/notpetya-ransomware-attack-cost-shipping-giant-maersk-over-200-million/#2b9eac584f9a (accessed February 19, 2020).

Michigan.gov. “Michigan Cyber Civilian Corps.” SOM. https://www.michigan.gov/som/0,4669,7-192-78403_78404_78419---,00.html (accessed May 19, 2020).

National Highway Traffic Safety Administration (NHTSA). Technology & Innovation. March 16, 2018. https://www.nhtsa.gov/technology-innovation. https://www.nhtsa.gov/technology-innovation (accessed May 15, 2020).

National Highway Traffic Safety Administration (NHTSA). Cybersecurity Best Practices for Modern Vehicles. October, 2016. (Report No. DOT HS 812 333). https://www.nhtsa.gov/sites/nhtsa.dot.gov/files/documents/812333_cybersecurityformodernvehicles.pdf (accessed January 30, 2020)

National Institute of Standards and Technology (NIST). “Cybersecurity Framework,” Updated May 21, 2020. http://www.nist.gov/cyberframework/ (accessed May 22, 2020).

National Institute of Standards and Technology (NIST). Framework for Improving Critical Infrastructure Cybersecurity. Version 1.1, April 16, 2018. https://nvlpubs.nist.gov/nistpubs/CSWP/NIST.CSWP.04162018.pdf (accessed December 19, 2019).

National Institute for Standards and Technology (NIST). Information Security Handbook: A Guide for Managers. October 2006. https://csrc.nist.gov/publications/detail/sp/800-100/final

National Institute of Standards and Technology (NIST). “The Five Functions.” (accessed February 28, 2020). https://www.nist.gov/cyberframework/online-learning/five-

functions (accessed February 28, 2020).

National Institute of Standards and Technology (NIST). “Framework for Improving Critical Infrastructure Cybersecurity.” February 2014. https://tsapps.nist.gov/publication/get_pdf.cfm?pub_id=915476 (accessed December 19, 2019).

NuHarbor Security. “Information Security Staffing Guide.” March 15, 2019. https://www.nuharborsecurity.com/information-security-staffing-guide . (accessed May 1, 2020).

Obama, Barack. Presidential Policy Directive-8. Washington, D.C.: The White House, March 30, 2008.

Obama, Barack. Presidential Policy Directive-21. Washington, D.C.: The White House, February 12, 2013.

Obama, Barack. Executive Order-13618. Assignment of National Security and Emergency Preparedness Communication Functions. *77 FR40779.* July 6, 2012.

Obama, Barack. Executive Order-13636. Improving Critical Infrastructure Cybersecurity. *78 FR 11737*. February 19, 2013.

Obama, Barack. Executive Order-13691. Promoting Private Sector Cybersecurity Information Sharing. *80 FR 9347*. February 20, 2015.

PCI Security Standards Council®. “PCI Security.” https://www.pcisecuritystandards.org/pci_security/ (accessed May 20, 2020).

Payment Card Industry (PCI) ®. “PCI Security.” Version 1.0, 2019. https://www.pcisecuritystandards.org/documents/PCI-Secure-Software-Standard-v1_0.pdf (accessed May 20, 2020).

Price Waterhouse Coopers. Global State of Information Security® Survey 2018. https://www.pwc.com/us/en/services/consulting/cybersecurity/library/information-security-survey.html (accessed May 20, 2020).

Pompon, Raymond, Debbie Walkowski, Sara Boddy, and Mike Levin. “2018 Phishing and Fraud Reports: Attacks Peak During the Holidays.” F5 Labs. November 8, 2018. https://www.f5.com/labs/articles/threat-intelligence/2018-phishing-and-fraud-report--attacks-peak-during-the-holidays (accessed January 24, 2020).

Roman, Alex. “Q&A with APTA Chair and JTA CEO Nathaniel P. Ford Sr.” *METRO*, February 12, 2018. https://www.metro-magazine.com/mobility/article/728416/q-a-with-apta-chair-and-jta-ceo-nathaniel-p-ford-sr (accessed February 28, 2020).

Security Boulevard. “10 Statistics that Summarize the State of Cybersecurity in Financial Services.” November 12, 2019. https://securityboulevard.com/2019/11/10-

statistics-that-summarize-the-state-of-cybersecurity-in-financial-services/ (accessed May 1, 2020).

Siegel, Jim. “An Ohio Cybersecurity Reserve Could Soon Respond to Network Emergencies.” *Government Technology*, September 18, 2018. http://www.govtech.com/security/An-Ohio-Cybersecurity-Reserve-Could-Soon-Respond-to-Network-Emergencies.html (accessed May 19, 2020).

Slaby, James R. “Ransomware Still Threatens the Transportation and Logistics Industry.” Acronis. https://www.acronis.com/en-us/articles/ransomware-logistics/ (accessed January 20, 2020).

Transportation Research Board. *Protection of Transportation Infrastructure from Cyber Attacks: A Primer.* Washington, D.C.: The National Academies Press, 2016. DOI: 10.17226/23516

Transportation Security Administration (TSA). Security Training for Surface Transportation Employees. 49 CFR 1570.201. March 23, 2020. https://www.federalregister.gov/documents/2020/03/23/2020-05126/security-training-for-surface-transportation-employees

Transportation Security Administration (TSA). “Mission.” https://www.tsa.gov/about/tsa-mission (accessed March 13, 2020).

Transportation Security Administration (TSA). “Cybersecurity Roadmap 2018.” November 2018. https://www.tsa.gov/sites/default/files/documents/tsa_cybersecurity_roadmap.pdf (accessed May 15, 2020).

Transportation Security Administration (TSA). “TSA Releases Cybersecurity Roadmap.” December 4, 2018. https://www.tsa.gov/news/releases/2018/12/04/tsa-releases-cybersecurity-roadmap (accessed March 13, 2020).

Trump, Donald J. Executive Order-13800. Strengthening the Cybersecurity of Federal Networks and Critical Infrastructure. *82 FR 22391*. May 16, 2017.

Trump, Donald J. Executive Order-13873. Securing the Information and Communications Technology and Services Supply Chain. *84 FR 22689*. May 17, 2019.

United States Senate, Committee on Armed Services. Inquiry into Counterfeit Electronic Parts in the Department of Defense Supply Chain, 112 Congress, 2nd Session, Report 112-167. May 21, 2012. https://www.armed-services.senate.gov/imo/media/doc/Counterfeit-Electronic-Parts.pdf (accessed April 7, 2020).

United States Senate. S.1760 National Defense Authorization Act for Fiscal Year 2020, Section 7613, 116th Congress. https://www.congress.gov/bill/116th-congress/senate-bill/1790/text (accessed April 7, 2020).

ABOUT THE AUTHORS

SCOTT BELCHER, JD, MPP

Scott Belcher is the President and CEO of SFB Consulting, LLC, where he specializes in transportation, transportation technology, the internet of things, smart cities, and the environment. Prior to his role at SFB Consulting, Mr. Belcher served as the CEO of the Telecommunications Industry Association for two years and the President and CEO of the Intelligent Transportation Society of America (ITS America) for seven years. Mr. Belcher has more than 35 years of private and public sector experience in Washington, D.C. Before joining ITS America, Mr. Belcher held senior management positions at a number of prominent trade associations, worked in private practice at the law firm of Beveridge & Diamond, PC, and served at the U.S. Environmental Protection Agency. Mr. Belcher serves on a number of public and private advisory boards. Mr. Belcher holds a JD from the University of Virginia, a Masters of Public Policy degree from Georgetown University, and a Bachelor of Arts degree from the University of Redlands in Redlands, California.

TERRI BELCHER

Terri Belcher is a writer and analyst who has worked in Washington, D.C. for the past 30 years. Ms. Belcher has 20+ years of experience working as a policy analyst and writer for the federal government, federal contractors, and numerous non-profits. Ms. Belcher earned a Bachelor of Arts degree from the University of Redlands in Redlands, California.

ERIC GREENWALD, JD

For the last four years, Eric Greenwald has been the General Counsel of Redacted, a cyber security firm based in San Francisco, CA. He joined Redacted from the White House, where he served as the Special Assistant to the President & Senior Director for Cybersecurity on the National Security Council (NSC). At the NSC, he was charged with coordinating cybersecurity efforts across the federal government on matters of international policy, national security, intelligence, law enforcement, and incident response. Prior to his work at the White House, Eric served as the Principal Deputy Director of the FBI's National Cyber Investigative Joint Task Force and as the Deputy Director of Operations at U.S. Cyber Command, where he provided legal and policy guidance to senior leadership on defensive and offensive cyber operations. Eric also worked on Capitol Hill as Chief Counsel for the House Permanent Select Committee on Intelligence and served as an Attorney Advisor with the CIA's Office of General Counsel.

In the private sector, he worked as a litigator and an international trade lawyer with the law firms Steptoe & Johnson and Shearman & Sterling. More recently, he worked as an associate producer for the CBS News program "60 Minutes" and as an editor for National Public Radio. Mr. Greenwald received his bachelor's degree in international relations from Yale University and his law degree from the University of Michigan Law School.

BRANDON THOMAS, MBA

Brandon Thomas is a Partner at Grayline Group, a firm focused on helping organizations understand and manage for disruption, as well as a Managing Partner of Blockview Partners, a firm focused on understanding the emerging blockchain and cryptocurrency space. Mr. Thomas has worked in both startup and corporate environments as he discovered his passion for working among disruptions. Mr. Thomas co-wrote the initial data strategy Democratic National Committee that went on to revolutionized campaign politics. He was employee #1 at one of the first software-as-a-services (SaaS) startups in the HR space. More recently, Mr. Thomas has been working on behalf of clients to understand the disruption afoot in the public transit industry. He is co-author of "Chain Reaction: How Blockchain Will Transform the Developing World," to be published by Palgrave Macmillan in autumn 2020. From the rise of data in politics to the emergence of SaaS to the ubiquitous nature of social media to the emerging blockchain and cryptocurrency realm, Mr. Thomas has worked to build numerous businesses to understand and exploit opportunities spurred by ever-increasing technological change. Brandon received his BA from The George Washington University and his MBA from the University of Texas at Austin.

PEER REVIEW

San José State University, of the California State University system, and the Mineta Transportation Institute (MTI) Board of Trustees have agreed upon a peer review process required for all research published by MTI. The purpose of the review process is to ensure that the results presented are based upon a professionally acceptable research protocol.

MTI FOUNDER

Hon. Norman Y. Mineta

MTI BOARD OF TRUSTEES

Directors

MINETA TRANSPORTATION INSTITUTE