7-2022

Aligning the Transit Industry and Their Vendors in the Face of Increasing Cyber Risk: Recommendations for Identifying and Addressing Cybersecurity Challenges

Scott Belcher
Mineta Transportation Institute

Terri Belcher
Mineta Transportation Institute

Kathryn Seckman
Mineta Transportation Institute

Brandon Thomas
Mineta Transportation Institute

Homayun Yaqub
Mineta Transportation Institute

SJSU SAN JOSÉ STATE UNIVERSITY

MTI MINETA TRANSPORTATION INSTITUTE

Aligning the Transit Industry and their Vendors in the Face of Increasing Cyber Risk: Recommendations for Identifying and Addressing Cybersecurity Challenges

Scott Belcher
Terri Belcher
Kathryn Seckman
Brandon Thomas
Homayun Yaqub

Mineta Transportation Institute

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 Mineta Consortium for Transportation Mobility (MCTM) funded by the U.S. Department of Transportation and the California State University Transportation Consortium (CSUTC) funded by the State of California through Senate Bill 1. MTI focuses on three primary responsibilities:

Research

MTI conducts multi-disciplinary research focused on surface transportation that contributes to effective decision making. Research areas include: active transportation; planning and policy; security and counterterrorism; sustainable transportation and land use; transit and passenger rail; transportation engineering; transportation finance; transportation technology; and workforce and labor. MTI research publications undergo expert peer review to ensure the quality of the research.

Education and Workforce

To ensure the efficient movement of people and products, we must prepare a new cohort of transportation professionals who are ready to lead a more diverse, inclusive, and equitable transportation industry. To help achieve this, MTI sponsors a suite of workforce development and education opportunities. The Institute supports educational programs offered by the Lucas Graduate School of Business: a Master of Science in Transportation Management, plus graduate certificates that include High-Speed and Intercity Rail Management and Transportation Security Management. These flexible programs offer live online classes so that working transportation professionals can pursue an advanced degree regardless of their location.

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 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 22-30

Aligning the Transit Industry and their Vendors in the Face of Increasing Cyber Risk: Recommendations for Identifying and Addressing Cybersecurity Challenges

Scott Belcher

Terri Belcher

Kathryn Seckman

Brandon Thomas

Homayun Yaqub

July 2022

A publication of the
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. 22-30	**2. Government Accession No.**	**3. Recipient's Catalog No.**	
4. Title and Subtitle Aligning the Transit Industry and Their Vendors in the Face of Increasing Cyber Risk: Recommendations for Identifying and Addressing Cybersecurity Challenges		**5. Report Date** July 2022 **6. Performing Organization Code**	
7. Authors Scott Belcher, 0000-0002-5843-1538 Terri Belcher, 0000-0002-9355-4357 Kathryn Seckman, 0000-0003-0177-1715 Brandon Thomas, 0000-0002-7986-2716 Homayun Yaqub, 0000-0001-7363-5443		**8. Performing Organization Report**	
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 State of California SB1 2017/2018 Trustees of the California State University Sponsored Programs Administration 401 Golden Shore, 5th Long Beach, CA 90802		**13. Type of Report and Period Covered** **14. Sponsoring Agency Code**	
15. Supplemental Notes			
16. Abstract Public transit agencies in the United States depend on external vendors to help deliver and maintain many essential services and to provide critical technologies, from ticket purchases to scheduling to email management. While the integration of new, advanced technologies into the public transit industry brings important advancements to U.S. critical transportation infrastructure, the application of digital technologies also brings with it a new assortment of digital risks. Transit agencies of all sizes are finding themselves subject to cyber incidents—most notably ransomware attacks—like those experienced by larger, more prominent companies and critical infrastructure providers. The findings in this report focus on helping all parties involved improve in three key areas: cyber literacy and procurement practices, the lifecycle of technology vis-à-vis transit hardware, and the importance of embracing risk as a road to resiliency.			
17. Key Words Cybersecurity, Ransomware, Public Transit, Cyber attack, Enterprise Risk Management.	**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** 71	**22. Price**

Form DOT F 1700.7 (8-72)

DOI: 10.31979/mti.2022.2113

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/research/2113

CONTENTS

LIST OF FIGURES

Executive Summary

The integration of new technologies into the public transit industry has resulted in improved service offerings to customers. But while these new services provide important information and conveniences to transit customers, they may also provide access points for nefarious actors who want to disrupt or cripple operations. As in other industries, the increased application of digital technologies in public transit (*e.g.,* service delivery, customer interactions, and back-office operations) brings with it a new assortment of digital risks. Unfortunately, many U.S. public transit agencies are not prepared for these risks.[1] Transit agencies of all sizes have found themselves subject to cyber incidents, most notably ransomware attacks that resemble those experienced by larger, more prominent companies and critical infrastructure providers. The transit industry needs to expand and mature its cyber preparedness in a timely manner but is unlikely to be able to do so without assistance.

U.S. transit agencies are highly dependent on the services of external vendors to help in the delivery and maintenance of many critical technologies linked to everything from ticket purchases to scheduling to email management. A vendor's cybersecurity posture—whether immature or advanced—is shared with its clients. The transit industry and its vendor community have the opportunity to broaden their mutually beneficial relationships with a focus on cybersecurity. In this case, both parties need to create security environments that benefit from and augment each other.

The authors of this report conducted interviews with key vendors in the public transit industry with the intention of learning more about the current state of cyber security in public transit from the vendor perspective, how this translates to contractual requirements and service delivery, and how operators can become more cyber-savvy clients. Our findings, which are presented in an anonymized fashion, focus on three key areas: cyber literacy and procurement practices, the lifecycle of technology vis-à-vis transit hardware, and the importance of embracing risk as a road to resiliency.

Many vendors remarked in their interviews that transit agencies need to use the procurement process as an opportunity to clearly articulate their cyber expectations and needs because the presence of such requirements in requests for proposals (RFPs) is a key driver of investment for vendors. It is important, however, that agencies have a sense of their own risks and have the ability to communicate these risks in technical terms that align with the actual needs of the organization or service delivery being sought from the vendor. Keeping technical teams, especially security personnel familiar with agency cyber requirements, integrated into the procurement process is one way to address some of these hurdles.

Transit vendors were nearly unanimous in their observation that the hardware and software lifecycles in public transit are out of sync, creating a situation in which vehicles and other hardware designed to last for 15 years or more are being supported by or carrying software that stopped receiving security updates five years after it launched. This disconnect creates serious

vulnerabilities. Transit agencies need to not only be on the lookout for software and firmware that is obsolete and unsupported (and seek to remove or replace it as quickly as possible), but also explicitly cite the need for vendors to provide ongoing service in RFPs. Agencies should anticipate increased costs in the near term, but planning to avoid technology obsolescence is a worthwhile security investment.

Finally, vendors acknowledged the importance of viewing organizational needs through lenses that focus on risk and security and how understanding the difference is foundational for addressing cyber risks. Security is a state of being which organizations take steps to protect themselves—essentially creating an environment free from or resilient against harm. Risk, on the other hand, is something that organizations would do well to accept as a constant chance or probability of exposure to hazards. Risk is managed or mitigated to the extent possible, but it generally cannot be eliminated. This mindset would not only help transit agencies in their own cyber risk management but also positions them to gain more from their relationships with vendors.

The most impactful step a transit operator can take to strengthen their cyber resiliency is to consolidate and elevate risk management as a core function of the organization that incorporates all elements of risk, including cyber, into a single, focused effort. Known broadly as an enterprise risk management (ERM) strategy, risk consolidation allows for the organization to operate as a united front against the myriad risks that confront it daily. Taking this concept of an organizational approach and broadening it to a whole-of-industry approach would provide benefits to all stakeholders involved in ensuring public transit's future success. The macro areas of focus for ERM include people and process (who and how risk is managed), technology (by what means), and governance (why and how risk should be managed).

There is a growing urgency for expanded regulatory guidance and directives regarding cybersecurity for U.S. critical infrastructure, including public transit. A Transportation Security Administration (TSA) Security Directive released in December 2021 specifically addressed cyber for rail systems and was accompanied by a recommendation that other surface transportation operators follow the directive as well. The authors anticipate that recent recommendations may evolve into future directives as the government continues to mature its regulatory approach to information security practices in the public and private sectors.

Finally, the report concludes with an outline of actionable steps that each of the key transit stakeholders can and should be taking to help shore up the industry's cyber maturity and ability to counter today's cyber risks. Vendors, transit agencies, transit associations, and the U.S. Government all need to make targeted investments of time and resources to improve the cyber resilience of U.S. public transit.

1. Introduction

The U.S. public transit industry is in need of a twenty-first century security upgrade. Safety and security are at the forefront of operations today, but generally do not address the wide-ranging digital enhancements the industry is experiencing. Digital risks and exposure have grown as agencies incorporate new technologies into all areas of their business, including service delivery, back-office operations, customer interactions, and a multitude of third-party partnerships on which agencies rely to keep the organization's day-to-day operations in motion.

In this report, the authors present the findings of their research into the interface between public transit agencies and their vendors regarding cybersecurity and risk management practices. This builds on the work presented in the 2020 Mineta Transportation Institute (MTI) study, *Is the Transit Industry Prepared for the Cyber Revolution? Policy Recommendations to Enhance Surface Transit Cyber Preparedness* (2020 MTI Study), in which the authors reported on the growing technology demands within the industry and the resulting exposure to myriad cybersecurity threats for which most operators are unprepared.[2]

The findings of the 2020 MTI Study and research to date underscore the need for the public transit ecosystem in its entirety (*e.g.,* the agencies, vendors, trade associations, and regulatory bodies) to elevate its collective understanding of and preparedness for cyber-related risks to operations, data, and business infrastructure. Given the dependence transit agencies have on vendors and the role and reach vendors have in delivering technology and services, the focus of this paper is on the opportunities that exist for the industry to enlist the help of the vendor community to support the improvement of cyber risk management and the steps transit agencies need to take in order to create an environment that is able to collaborate with vendors.

Cybersecurity / The art of protecting networks, devices, and data from unauthorized access or criminal use, as well as the practice of ensuring confidentiality, integrity, and availability of information.

Based on follow-on research from the 2020 MTI Study, extensive interviews with vendors serving the transit industry and the ever-evolving cyber threat landscape, the authors have assembled a report designed to introduce or reacquaint readers with cyber risks posed to public transit agencies, the expansiveness of the vendor community supplying hardware and software, and a vendor-led view of cyber practices in transit. The latter half of the report focuses on the need for transit agencies to implement risk management practices as an avenue for strengthening their respective cyber capabilities and the U.S. regulatory environment that is nipping at the heels of transit, spurred on by high profile cyber-attacks against U.S. critical infrastructure by foreign actors. Finally, the authors offer a series of recommendations tailored to each of the stakeholders with a role to play in maturing cyber risk management capabilities in public transit.

2. Methodology

This report employed a multifaceted approach to research and document the status of public transit agencies and their primary vendors 'cyber readiness with the goal of developing practical recommendations to enhance those levels of preparedness. The report focused primarily on vendors that work with public surface transit agencies that receive funding from the Federal Transit Administration (FTA), are members of the American Public Transportation Association (APTA), and operate within the U.S.

2.1 Literature Review

The authors reviewed available material from government agencies, including the Department of Homeland Security (DHS), the Cybersecurity and Infrastructure Security Agency (CISA), TSA, the Department of Defense (DoD), the National Institute of Standards and Technology (NIST), and the U.S Department of Transportation (U.S. DOT), as well as trade associations such as the American Public Transportation Association (APTA), the American Association of State Transportation and Highway Officials (AASHTO), and the National Academies of Sciences ' Transportation Research Board (TRB). We also looked at best practices from other industries. The authors supplemented the literature review with open-source research on 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. The authors also attended and participated in several conferences, including the 2021 APTA TRANSForm Conference, 2021 APTATech Conference, 2021 California Transit Association Annual Meeting, 2021 ITS World Congress, 2021 AASHTO Annual Meeting, 2021 ITS America Annual Meeting, and 2022 TRB Annual Meeting.

2.2 Review of Best Practices

The authors reviewed literature on physical and digital cybersecurity strategies in transit and other industries and applied key findings from this review, as well as discussions with experts from both operators and vendors, to develop the oral survey guide that was used to gather information for this report. The researchers profiled the leading vendors as well as a number of companies in other industries to level set current actions and identify best practices that can be shared with the vendor community as well as operators.

2.3 Expert Interviews

With this background in place, the researchers worked with several transit operators to define the key enterprise areas that are exposed to the highest level of cybersecurity risk and where they rely on vendors to support these operations. Based on this input, the researchers focused on three primary enterprise areas: bus operations technology, fare payment technology, and transit business operations technology. The researchers assembled a list of large and small companies that provide

support services to these enterprise areas and worked with APTA and its Business Members Board of Governors (BMBG) to identify representative firms that might be willing to participate in in-depth interviews. The researchers, with the support of APTA and the BMBG, sought in-depth interviews with this target list and conducted interviews with suppliers providing the majority of the services in these enterprise areas. Additionally, the researchers interviewed multiple public agencies, trade associations, and Capitol Hill representatives.

Each interview included at least two researchers. With respect to the vendor interviews, the researchers sought to hold interviews with the Chief Information Security Officer (CISO)/Chief Technology Officer (CTO) (or top technology profession responsible for managing the organization's cybersecurity practices) and the top business development professional/technology professional who deals with clients on their cybersecurity needs, if different. In the interview process, the authors used scripted questions with each organization, though the discussion was otherwise unstructured, which enabled the authors to explore specific experiences and anecdotes that the interview subjects were able to share. A copy of the interview questions is attached as Appendix C. To ensure a high level of openness and candor, the interviews were conducted on an anonymous basis and a specific company or individual was only referenced with their permission.

2.4 Operational Recommendations

The report makes a series of recommendations for transit operators, transit vendors, the federal government, and other industry actors on how to best refine their relationships to introduce more rigor into their cybersecurity practices. The recommendations provide examples for how vendors can mature their cybersecurity practices and provide agencies with guidance on how their contracts and other practices can be employed to ensure clear expectations are conveyed to vendors. Neither agencies nor their vendors alone can fully mitigate cybersecurity risk. The industry must work together to address the growing threats to public transit that cyber-attacks pose.

2.5 Limitations of Study

The intent of this study is to assess the readiness, resources, and structure of public transit agencies and their suppliers to identify, protect from, detect, respond to, and recover from cybersecurity vulnerabilities and threats.[3] Further, while the authors provide a description of the threats currently facing the transit industry and their vendors, they did not specifically assess and 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. The authors did not assess the internal cybersecurity capabilities of any transit agency, vendor, or public organizations with whom many agencies share data, such as trade associations and/or federal agencies such as the U.S. DOT or DHS.

3. State of Play: Cyber Risk in Public Transit

The past several years have proven to be marquee years for cyber-attacks against critical infrastructure, including public transit agencies across the United States and Canada. Headlines in 2020 and 2021 called out only a fraction of the costly disruptions and security breaches governments and businesses experienced due to cyber-attacks. The 2021 Log4j vulnerability, Colonial Pipeline ransomware attack, JBS Foods hack, Kaseya software attack, and the 2020 SolarWinds attack are some examples, along with many others which disrupted systems, software, operations, and services, costing companies and governments exorbitant sums of money to clean up the mess.

IBM, in its 2021 *Cost of a Data Breach Report,* cited a 10% year-over-year increase in the average total cost of a data breach, placing the 2021 average at $4.24 million; the average total cost of a ransomware breach was $4.62 million (not including the cost of the ransom). These are the highest average total costs in the 17-year history of the IBM Security report.

Case Study: Ransomware Attack on Mid-Sized Public Transit Agency

One Friday before a long weekend in 2021, a mid-sized transit agency on the East Coast of the United States received a message that their system had been compromised by an outside actor, that their data was no longer accessible, and that a ransom demand would be forthcoming. The transit agency's IT team responded swiftly, though with the incorrect assumption that they could quickly turn to backups of their files and data to resolve the inconvenience. Unfortunately, the sophistication of the hackers and the thoroughness with which the transit operator's system was hijacked meant that neither the agency nor its cadre of vendors could tackle the data breach in a timely manner. What began as a minor disruption turned into a multi-week affair involving professional ransom negotiators, lawyers, and public relations experts.

A vendor providing management services to the transit agency was immediately brought into the incident in the hopes that they could assist the team in its response. The agency needed help sifting through more than 50 file servers to determine the kinds of data the hackers had in their possession. The servers were a mix of modern and legacy systems, with the legacy systems containing personal data on thousands of pensioners. Without an understanding of who and what would be harmed by the public release of the agency's data (the hackers had threatened to dump the data cache on the dark web), the team had no ability to conduct an effective risk assessment or take mitigating steps. The IT team, in the midst of it all, had unfortunately shut down all the systems, assuming this would limit additional harm. Instead, this further constrained the assessment process and the agency's ability to continue delivering uninterrupted back-office services. It was a scramble and expensive learning experience for all involved.

Following the incident, the vendor reflected that it took for granted that the transit agency had in place current policies, procedures, and contingencies to provide for cybersecurity. It was an incorrect assumption. Despite healthy funding from the state's Department of Transportation (DOT) for new electric and autonomous technologies, sufficient funds were not made available to maintain and upgrade existing systems. Given the size and scope of the agency's needs, annual requests for funding to modernize the agency's systems could not be fully met. As a result, neither the state DOT nor the transit agency were making adequate investments to address the growing cyber risks associated with the agency's technologies and data collection.

The agency was able to retrieve its data (though some of it was corrupted), albeit at a great expense in terms of time and money. All it took was an errant click on a single phishing email to bring normal operations to a screeching halt and put the agency's lack of a business continuity plan and cyber know-how on full display to its partners.

Public transit providers are seeing a similar uptick in the frequency and severity of cyber incidents. The global transit industry, according to Check Point Research, has experienced a 186% year-over-year increase in weekly ransomware attacks since June 2020.[4] The Bay Area Rapid Transit

system, Southeast Pennsylvania Transportation Authority, Vancouver's Translink, the Toronto Transit Commission, O'ahu Transit Services in Honolulu, New York's Metropolitan Transportation Authority, Dallas Area Rapid Transit, Ann Arbor Area Transportation Authority, and the Santa Clara Valley Transportation Authority in California have each dealt with their own data breaches or ransomware attacks in the past few years. It is increasingly difficult to name a transit provider that has not faced a data breach or other disruptive cyber incident. In some cases, transit agencies report clean cyber bills of health only because they are unaware of system breaches. Neither the size nor the location of the transit agency makes the operator immune to attack. Perpetrators of ransomware attacks on transit agencies are generally looking for financial payouts—it is a business operation.

The public transit industry is also accelerating its adoption of digital technologies. Consumer demands and expectations are changing significantly, driven in large part by consumer transactions with other sectors and industries as the opportunity to improve how service is delivered continues to grow. In public transit, a passenger increasingly begins their journey by reviewing schedules or status of transit vehicles through a web-based portal or app. The app is also becoming a method for purchasing an e-ticket, either validated as proof-of-purchase by a human conductor or through a verification system on the conveyance.

Transit agencies are also becoming increasingly dependent on this connectivity to manage their operations, from scheduling to depot parking and overall traffic management. As the industry accelerates the use of first and last mile services and Connected and Automated Vehicles (CAV), the digital interaction will only increase between the passenger and the broader ecosystem of devices and applications that provide the service of moving people.

The delivery and management of transit operations are increasingly reliant on a highly connected and cyber-dependent environment that is no longer bound by a self-contained network. Each connected point of interaction that makes use of the internet for the exchange of information is a vulnerable point of entry and may include, but is not limited to, passenger personal data, credit card information, conveyance location data, and conveyance/depot status. It is also important to note that this ecosystem extends beyond the passenger and transit provider; it includes the diverse collection of vendors—service, hardware, and software providers—upon which the agencies are dependent to fulfill their mandate. The vendor thus becomes more than a commodity purveyor; they are entrusted with providing technologies that are critical to performing the agency's mission.

Figure 1: Threats to Transit Sector Value Chain[5]

VALUE CHAIN PROCESS	STATE CYBERTHREAT ACTORS	CYBERCRIMINAL GROUPS	HACKTIVIST GROUPS	INSIDERS
Planning and Scheduling	• Theft of intellectual property • Targeted surveillance and monitoring	• Ransomware attacks to disrupt processes for financial gain • Theft of employee PII for sale or extortion	• Disclosures and embarrassment • Theft of travel plans and data • Disruption of expansion • Reputational damage	• Theft of intellectual property • Human error • Insider trading • Data monetization
Pricing and Ticket Sales	• Theft of client PII for espionage • Loss or corruption of critical client information • Loyalty or partner network data theft	• Ransomware attacks to disrupt processes for financial gain • Theft of client PII for use or resale • Credit card skimming	• Denial of service attack • Website defacement • Reputational damage	• Disruption or misuse of systems • Human error • Insider trading • Data monetization • Theft of funds
Station Operations (Wi-Fi, maintenance, etc.)	• Social disruptions • Interception of public Wi-Fi • Defacement of announcement boards	• Ransomware attacks to disrupt processes for financial gain • Interception of public Wi-Fi	• Disruption of operations through cyber- and physical attacks • Defacement of announcement boards • Reputational damage	• Human error • Disruption of processes • Theft of data or funds • Defacement of announcement boards • Reputational damage
Transit Operations	• Theft of system maintenance data • Cyberhijacking • Geolocation data disruptions • Sensor disruptions	• Ransomware attacks to disrupt processes for financial gain	• Disruption of travel • Panic-mongering • Reputational damage	• Disruption of processes • Theft of assets • Human error
Assets and Logistics	• Impact on route availability • Social disruption	• Ransomware attacks to disrupt processes for financial gain		

3.1 Vendor Community Serving Public Transit

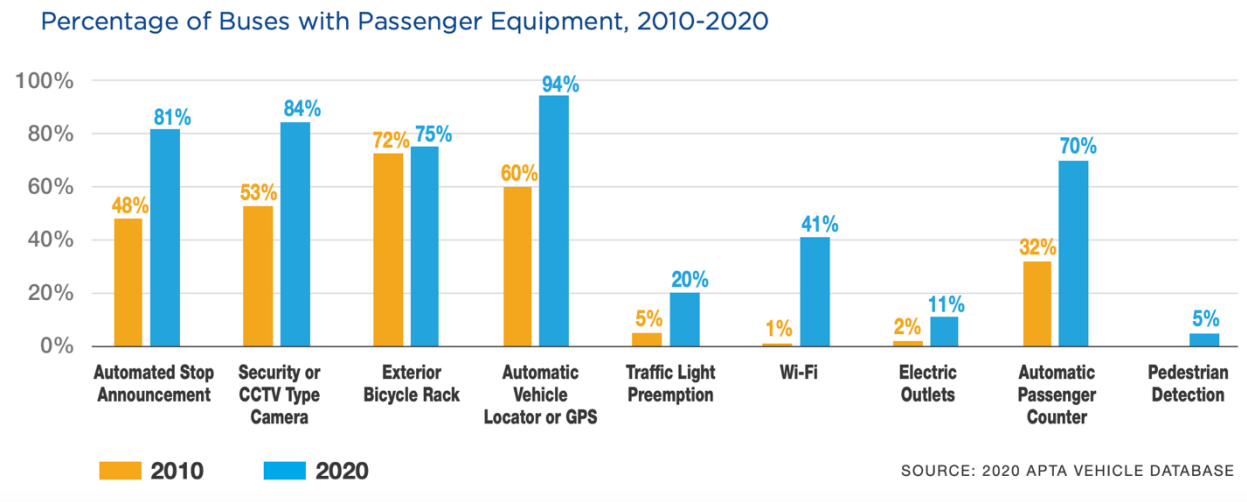
The role vendors play in delivering public transit services varies by agency, but all rely on the vendor community to provide technical support in some form. Public transit agencies are highly dependent on these services from external vendors, both to ensure the consistent and reliable delivery of transportation services and for the general operations of the agency. Some have outsourced much or all of their operations; others maintain some in-house capabilities to manage day-to-day technical needs. Agencies generally rely on vendors for Intelligent Transportation Systems (ITS) or services that automate service delivery (*e.g.*, computer-aided dispatch, scheduling, passenger counting), back-office services (*e.g.*, the running of the transit agency—email, data storage), fare

management, and, of course, the manufacturing of the actual vehicles. Vendors are often providing some or all of the following services to their transit agency customers:

- Ticket Purchases
- Cloud Services
- Fleet Management
- HR Systems
- Passenger Counting
- Video Surveillance
- Yard Management
- Scheduling
- Driver ID/Bus Access Real-Time Arrival
- Fare Management
- Data Storage
- Vehicle Locations
- Email Management
- Cred Card Processing

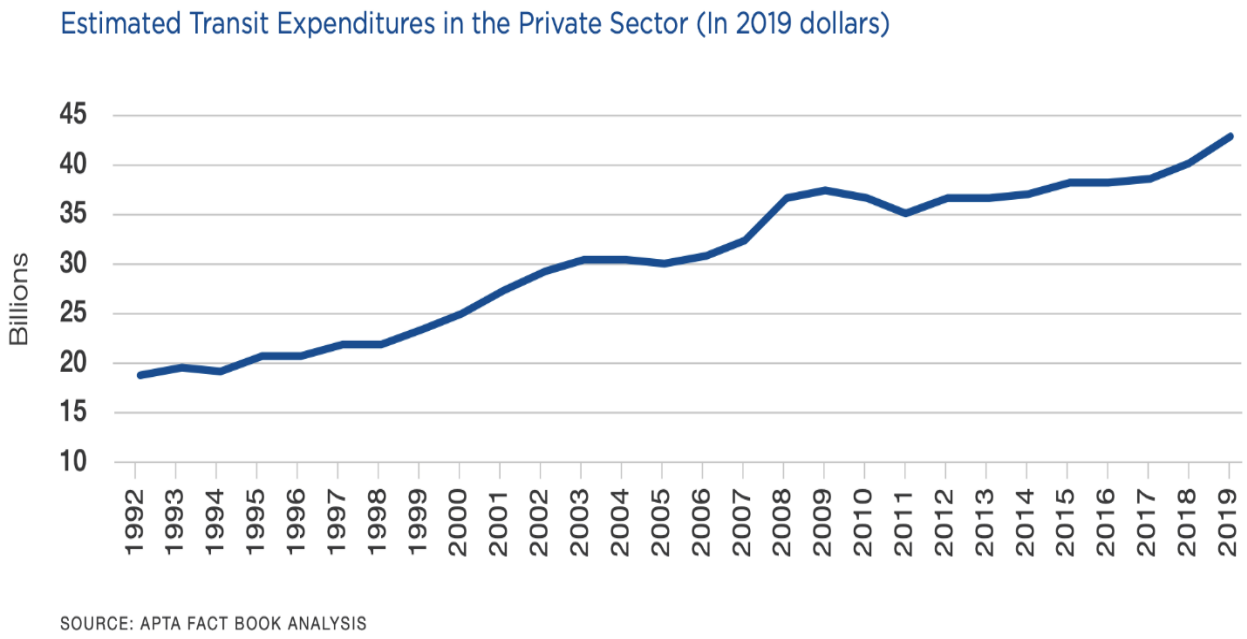
The APTA 2021 Fact Book provides another view on the growing use of technology in buses over the past 20 years. A review of the APTA figure illustrates a limited but demonstrative view of the increase in potential threat vectors being added to current buses.[6]

Figure 2: Transit Buses Continue to Add Amenities and Technology[7]



APTA also observes that "a large portion of the funds expended by those [public transportation] agencies, however, is spent in the private sector. In 2019, expenditures in the private sector were estimated at $43.1 billion (57 percent of all transit expenditures), a 7.5 percent increase from $40.1 billion in 2018 (inflation-adjusted)."[8] Given the historic increase in funding for transit in the Infrastructure Investment and Jobs Act (IIJA), this number is likely to increase exponentially.

Figure 3: Public Transit Expenditures Flow to Private Sector[9]



Vendors play an important cybersecurity role with regard to their work with transit clients. A vendor that has incorporated security as a core tenant of the service or product they deliver is, in turn, sharing that layer of security with their clients. Similarly, a vendor with nonexistent or

immature cybersecurity policies and practices can pass along that risk or exposure to their clients via their product or service. This often occurs without the client or vendor's knowledge.

Businesses serving the transit industry, however, are like other service businesses—they are going to be responsive to the wants and needs of their customers. If customers do not place value on security, it is unlikely to be a core component of either their sales pitch or the actual product/service delivery. In this regard, the transit industry and its supply chain have an opportunity to broaden their mutually beneficial relationships with a focus on cybersecurity.

3.2 Vendor Insights on Cyber Practices in Public Transit

Companies serving the public transit industry are in the beneficial position of learning their clients ' specific needs while also maintaining a wider view of the industry—what agencies of different sizes and in different regions need, how they use services, and what it is they are likely to request next. In a series of in-depth interviews the authors conducted with many of the largest transit industry suppliers in the U.S., vendors shared insights into the challenging relationships of industry expectations for cybersecurity, how this translates to interactions with the supply chain, and the recommendations cyber-proficient vendors have for individual agencies. Many of these vendors also provide products and services to companies outside the transit sector, which gives them cross-industry context and access to best practices the transit agencies may wish to adopt from more cyber-mature environments.

To protect the anonymity of the vendor companies that were interviewed, none of the anecdotes or feedback included in this section is cited or attributed to a specific individual or company. The authors have instead presented their aggregated findings and key themes from the interviews combined with actionable takeaways. Most of these actions and recommendations come directly from the vendors interviewed by the authors, who recognize that the quality of their service delivery and reputations depend on delivering some level of security—to the extent that they can—to their clients.

3.2.1 Cyber Literacy and Getting the Request for Proposal (RFP) Process Right

When asked specifically about their interactions with transit agencies, most vendors noted that many of the U.S. transit agencies with whom they work or to whom they submit proposals do not have the in-house cybersecurity know-how to clearly articulate their needs and expectations. Without a basic understanding of cyber risk within their agency, it is nearly impossible for a transit operator to adequately assess the product or service being procured and its impact on risk.

Overall, vendors are seeing an increasing number of RFPs that include cybersecurity provisions, albeit in an inconsistent and somewhat incoherent fashion. Several vendors noted in their interviews that the cyber requirements in many transit agency RFPs today are not a stretch for them to meet because the agencies have not yet reached a level of cyber sophistication that requires any major changes from vendors. While some vendors modified their cyber practices because they

serve other industries that hold vendors to a higher standard, many vendors acknowledged that their overall spend on cybersecurity had increased not due to client requests but because the business viewed it as an essential component of their own operations and enterprise risk.

Vendors shared multiple anecdotes about the range of cyber requirements among their transit clients. Some transit agencies, they noted, have limited or no cyber requirements or expectations in their RFPs. Others go into a level of detail in their requests, including requiring vendors to have specific certifications, which suggests that the RFP was assembled by an organization (perhaps even a third-party consultant) without the ability to align with the agency's internal understanding of risk (if established). In some cases, vendors noted, they are seeing agencies pursue security for security's sake without a rational understanding of risk. This is apparent in RFPs that include duplicative and often conflicting requirements.

In one case, a vendor received an RFP, for which they were otherwise well-qualified to bid on, that required vendors to have a FedRAMP certification. The FedRAMP certification goes well beyond the ISO 27001 and NIST 800-53 security and privacy controls that often serve as stepping stones to the management of more mature information systems

ISO 27001: An international standards body headquartered in Switzerland that provides a widely known set of requirements for information security management systems. Organizations can become certified to ISO 27001 standards.

NIST 800-53: The U.S. National Institute of Standards and Technology (NIST) Risk Management Framework provides a comprehensive process organizations can use to manage information security and privacy risk.

FedRAMP is considered one of the more difficult certifications to achieve and includes third-party assessment requirements as well as a review by a government authority. Companies providing cloud data storage services to the federal government are generally required to achieve this level of certification. From the vendor's perspective, the transit agency requesting FedRAMP certification as a condition of a successful bid did not have work that required that level of security, was not in possession of federal data, and did not have in-house security requirements or policies that could operate at that level of maturity. In short, the request for the FedRAMP certification for this work was an indication that the transit organization did not know what it needed, did not have a level of cyber literacy to communicate those needs in their RFP, and only served to unnecessarily increase the cost of the response.

Such disproportional asks cost time and money. There is no need for a transit agency to pay for a level of service it does not require. And FedRAMP certifications require frequent, ongoing maintenance. This is a worthy investment if it aligns with the organization's service delivery needs. In this case, however, it was being used as an expensive catchall in place of doing the work to understand the agency's risk profile. Any organization requiring its supply chain to maintain this

level of certification is going to have to pay for it. Similarly, vendors will have to make the business decision about whether the cost of bidding for an RFP, which may sometimes include upgrades to their own operations, is worth the investment.

Several of the vendors underscored their desire to see more informed cybersecurity requirements in agency RFPs. This will likely improve the cyber posture of the industry, but it also allows more mature vendors to distinguish themselves from their less cyber-mature competitors. Vendors making investments in cybersecurity are looking for returns on these investments (although one could argue that the improved security for their business and products is the primary ROI). The transit industry—given its dire need for assistance in better securing its operations from cyber threats—should reward those vendors that invest in and maintain reality-aligned cyber practices with contracts. Cybersecurity needs to become a business development tool that serves as a key differentiator among transit vendors. In parallel, agencies need to better educate themselves on information security capabilities such that they can make more informed decisions concerning their vendors.

The procurement process can be cumbersome, but a measured, deliberate, and thorough process is required to vet, validate, and otherwise ensure vendors meet necessary standards to serve public transit. An increased reliance on technology further underscores the central importance of getting the terms of these relationships right. Part of the challenge, as highlighted by the Transportation Research Board (TRB) in their 2022 study on Cybersecurity in Transit Systems, is that "there is no transportation-specific, let alone transit-specific, guidance to assist in developing a cyber secure procurement process and working with third-party software or vendors."[10]

Transit agencies have an opportunity during the public RFP process, multiple vendors noted, to secure services that incorporate modern cyber risk practices. Clearly stipulated cybersecurity requirements that are commensurate with the actual needs of the agency can go a long way in helping vendors to better serve transit clients, manage costs, and give transit agencies much needed support in their pursuit of managing cyber risk. The cyber requirements in RFPs are a key driver for investments in levels of compliance and certifications that vendors pursue to win contracts. Getting the language right from the start of the RFP, therefore, is not only important for ensuring that an agency gets what it needs, but it is also a means of improving an organization's cyber posture.

Agencies would also benefit from including a diverse team in the procurement process that, at minimum, includes security personnel familiar with cyber requirements. Agency visibility into the security practices of vendors is essential, especially if those vendors are to provide key systems or handle sensitive data.

It is important for the transit agency's leadership (technical or not) to work toward developing at least a basic level of cyber literacy. This education can be supported by vendors, but much of these learnings must be internalized by the agency, normalized for the industry, and integrated with the broader public transit ecosystem. The agency's technical teams must have a level of information

security knowledge such that they can engage in cyber-literate discussions, both in-house and with vendors. Even a basic understanding of cyber risk will enable better informed decision-making about the technology, people, and financial resources required to keep the agency functioning in a manner that aligns with its organization's risk tolerance.

3.2.2 Managing the Technology Lifecycle

Transit vendors were almost unanimous in their agreement that hardware and software lifecycles in public transit are out of sync. An agency, for example, may purchase several new buses for their fleet with the intent that those buses will have a lifecycle of at least 15 years. Traditionally, with good mechanics, the safety of the vehicle could be maintained for a long period of time. Today, the technology built into buses—everything from video cameras to location tracking—requires updates aligned to advances in technology and the ever-evolving list of threats that could undermine the security of their operations. The software and firmware used to manage and operate these devices, however, require updates on a timeline counted in months, not decades.

The result of misaligned lifecycles between hardware and software is that transit agencies are increasingly finding themselves the owners of technology for which vendors no longer provide security updates. If the lack of security updates did not have a direct link to passenger safety—the key driver for many technology investments in public transit—the lack of regular security updates would not be a priority. Keeping up with the latest tools of the technology industry is not a priority for many transit operations. The connection between the physical security of the vehicle and the digital technologies integrated into today's operations, however, means that the technologies present in the vehicles have a direct link to the security of passengers and others on the road.

This creates a conundrum for both the transit operator and the vendor. As vendors improve their products, investment and attention are primarily paid to the most recent and advanced iteration rather than coming up with solutions to secure a software package deployed a decade earlier. The transit operator, however, often needs to find a way to extend the life of software to service hardware that must last another five to ten years. If the software or firmware is no longer being updated by the vendor or is physically not able to be updated, the agency has a problem. Running software or a product with firmware that is not being updated means that previously unknown vulnerabilities may exist and *persist*. Hackers or other individuals looking to disrupt the transit service can exploit these vulnerabilities. Even updated software and firmware can have vulnerabilities, but managing cyber risk in this case is akin to securing a home. Someone can break into a home even if it has a moat, drawbridge, and Doberman, but it is going to be a lot more difficult, which may send them off in search of an easier target. The easier target is a home with an unlocked front door. The transit agency with software and firmware that is not being updated is the latter.

When technology advances at a rate that far outpaces public sector budget cycles and costly hardware investments, as the industry is experiencing today, changes need to be made to the agency-vendor contract terms and the expectations of both parties. The authors heard in multiple

interviews that vendors want to provide the best possible service to their transit customers, but the expectation to maintain software and firmware on anything other than a technology-driven timeline needs to be built into the contract such that the business can take steps to ensure they allocate the time and resources to do so.

Some vendors have realized this disconnect and have taken steps to build service agreements into their contracts. More service, however, leads to higher costs, especially with vendors that do not price in ongoing maintenance and updates. Transit agencies, therefore, need to explicitly cite the need for this level of ongoing service in their RFPs so that vendors can compete based on the actual required scope of work. It is equally important for agencies to incorporate the cost-of-service contracts into their budgets and capital planning.

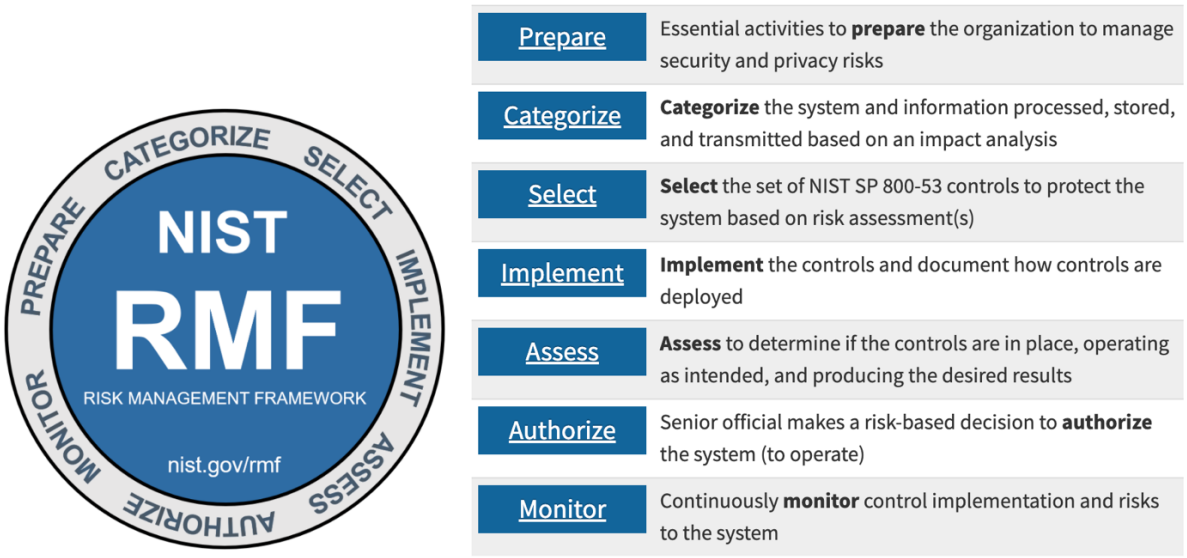
3.2.3 Managing Risk and Strengthening Resiliency

Multiple vendor interviews highlighted a core concept that many transit agencies could benefit from adopting—the importance for agencies to understand the difference between "security" and "risk" and how understanding the nuances of each can help an organization to improve its cyber posture. The line between the two concepts is thin, but it can ultimately impact how an organization chooses to prepare for or embrace the challenges of incorporating more technology and connectivity into its ecosystem.

Security is generally understood as a state of being free from or resilient to harm. The organization responsible for security at a transit agency today is most likely responsible for implementing policies and protocols designed to keep people safe—controlling points of access for buildings and vehicles, planning for and training people to respond to physical security incidents (bomb threats, physical altercations, etc.), among many other vital responsibilities.

If security is a state of being that organizations take steps to create, risk is the constant chance or probability of exposure to hazards in everyday life. Risk is something to be anticipated, analyzed, managed, and accepted. Steps can be taken to mitigate or reduce risk exposure to an individual or organization, but it generally cannot be eliminated from a situation. This is true for cyber threats as well.

Figure 4: NIST Risk Management Framework



When it comes to cyber risks faced by public transit agencies, there is no situation where an agency is absolutely free from danger or threat. As with most risks, cyber threats must be anticipated and managed, which can seem daunting for organizations that have not yet taken the steps necessary to bridge their traditional physical security practices with cyber risk management.

> Cyber resiliency// The ability to anticipate, withstand, recover from, and adapt to adverse conditions, stresses, attacks, or compromises on systems that use or are enabled by cyber resources.

The good news is that most public transit agencies already have recovery and response plans in place linked to threats posed by physical risks. Many operators are directly engaged in broader disaster planning for their respective cities, with responsibilities to help move people as evacuations are ordered in the face of natural or man-made disasters or community incidents. These plans are meant to ensure enterprise resiliency—anticipating what could occur, the likelihood of such an occurrence, and the potential resulting impact on the organization. Few of these plans, however, incorporate the potential impact of cyber risk.

Embracing a holistic approach to managing risk that is inclusive of and informed by physical, cyber, and information risks entails bringing what today are diverse elements of an organization together to reimagine an enterprise-wide view of risk.

The adoption of a risk strategy inclusive of cyber threats enables an agency to articulate its expectations for vendors—what a potential vendor needs to have in place in terms of security, how the organizations 'respective risk programs can complement one another, and what gaps may exist

that need to be addressed before contracts are signed. When an agency lacks a comprehensive understanding of its risk, it is very challenging for vendors to pinpoint where and how they can provide support. Consultants can assist in this process, but some vendors shared that inconsistencies in priorities exist when the definition of risk is not incorporated into organization-wide policies and procedures. Transit agencies will be in a much stronger position to secure their own operations and gain more from their vendor relationships when they take the steps needed to establish a holistic risk framework.

Case Study-Indiscriminate Cyberattacks: Community Services and Transit

A transit agency that provides essential transportation services to communities in need of economic assistance seems an unlikely target for a ransomware attack. Unfortunately, most cybercriminals do not discriminate based on an organization's size, stature, or the nature of the services they provide. They pursue access. In 2021, the seemingly unlikely victim of the cyber-attack was a transit provider in the eastern United States. The organization's systems were accessed via a suspected phishing attack.

As a result of the attack, the transit provider lost all of its historic and current route data, as well as client data. The agency's internal work product, emails, and other operating documents were stored on a second server that was also compromised. Although most of this data was not lost, it took months of unbudgeted overtime and consulting services to unencrypt the files. The organization decided not to pay the ransom, which left the agency to manually recreate their scheduling logs from paper manifests. The operator was left in the unenviable position of manually operating its schedule for months.

A system breach at this transit agency was seen as particularly unlikely by the leadership because of its affiliation with a Community Action Agency (CAA). CAAs are local, public, and private non-profit organizations that serve low-income communities by providing everything from transit services to early child development programs such as Head Start. As the Executive Director of this particular CAA mused, "we are the good guys, and we have nothing. Why would they hack us?" The associated transit agency in this case provides roughly 80,000 fixed-route, on-demand, and para-transit trips for individuals in need of access to essential services in the community.

When the transit agency's systems started shutting down, the CAA's IT staff began the process of shutting down the systems throughout the rest of the CAA. The entire organization was taken offline—cut off from emails, work products, scheduling software, financial software, and other daily business operational services. Fortunately, the non-transit CAA operations were on different servers than the transit operator's two on-premises servers, allowing them to isolate the hack and eventually restart other CAA systems.

The CAA is beginning to work with its employees to establish a cyber-awareness culture but is still in need of a comprehensive cyber assessment. The IT staff updated policies regarding passwords, authentication methodologies, and data access and is sending regular educational updates on cybersecurity scams, but there is still much more to be done. Competing priorities and limited resources appear to be stalling efforts by leadership to implement change. More solutions are needed to aid organizations like this CAA and their transit provider to improve cyber practices and discourage cybercriminals from viewing them as easy targets.

3.3 Managing and Mitigating Risk

One actionable takeaway from the research and interviews that were conducted for this report is that a vendor can have a robust risk management program to support their clients, but unless the client is able to take advantage of the vendor's work, risk is neither managed nor mitigated. The transit client must have a basic level of sophistication to integrate the risk program of the vendor into their own. To better position themselves to develop an integrated risk relationship with their vendors, transit agencies need to establish an understanding of their own risk posture that includes both cyber and physical risks. Socrates 'adage of "know thyself" is the best place for agencies to begin.

> **Enterprise Risk Management** (ERM) is defined by the Committee of Sponsoring Organizations (COSO) as "a process, effected by an entity's board of directors, management and other personnel, applied in strategy setting and across the enterprise, designed to identify potential events that may affect the entity, and manage risk to be within its risk appetite, to provide reasonable assurance regarding the achievement of entity objectives." COSO, since its inception in 1985, has provided thought leadership on risk management and governance among other topics related to the private and public sectors.

The authors believe the key to strengthening the broader transit ecosystem is a willingness to consolidate and elevate risk management as a core function of agency leadership, incorporating financial, operational, cyber, and other business risks into a single focused effort. Known broadly as Enterprise Risk Management (ERM), such a strategy ensures executive attention to improve cyber protections and preparedness to the same degree as other such risks are managed today.

There is a multitude of ERM resources transit agencies can consult to begin or advance industry and organization-specific needs and interests. Many of these are industry agnostic, though there are transit-specific materials under development. In the following text, the authors provide an overview of the macro elements of ERM as applied to transit agencies and, more specifically, how these elements apply to the agency-vendor relationship. The macro areas of focus include people and process, technology, and governance.

3.3.1 People and Process

ERM is a whole-of-organization approach that acknowledges the importance of managing risk not as a discrete set of actions, but as an integrated approach to reducing risk exposure that could otherwise negatively affect the organization and those they serve. Given the challenges of the industry and the growing threats it faces, the authors propose broadening the concept to a whole-of-industry approach, engaging agencies, vendors, and government to support the elevation of risk.

For most public transit agencies, a physical security team is responsible for providing security and risk management counsel to the organization's leadership. Many agencies already include "risk

management" in the job descriptions and/or titles of their existing security team; some even include cyber-related responsibilities. Technology, however, is most often managed by an entirely separate organization. This segmentation presents a challenge given the interplay between cyber systems and physical risk, and vice versa. Managing the connectivity between cyber risk and physical risk is not a native challenge to public transit or even the transportation sector writ large. Organizations of all sizes in every industry continue to iterate on the best way to manage this interface within their respective organizations. Referred to as the cyber-physical convergence, CISA and others have been researching and struggling to find answers for how to effectively manage this evolving risk landscape.

> Together, cyber and physical assets represent a significant amount of risk to physical security and cybersecurity—each can be targeted, separately or simultaneously, to result in compromised systems and/or infrastructure. Yet physical security and cybersecurity divisions are often still treated as separate entities. When security leaders operate in these siloes, they lack a holistic view of security threats targeting their enterprise. As a result, attacks are more likely to occur and can lead to impacts such as exposure of sensitive or proprietary information, economic damage, loss of life, and disruption of National Critical Functions (NCFs).[11]

Drawing from examples in financial services and energy, many organizations choose to unify and elevate the role of risk management to encompass both the physical and digital domains, often under a Chief Security Officer (CSO) or Chief Risk Officer (CRO). For some organizations, the most effective way to ensure that this individual and her team can lead a whole-of-enterprise approach to risk management is to have her report directly to the CEO. Other organizations have this individual report directly to another member of the C-Suite. The important factor is for this individual to have consistent visibility and access to leadership and the Board. As a member of the executive team, the CSO should serve as the focal point for all security matters, with a focus on ensuring compliance with agency guidance, maintaining and improving their organization's security posture and readiness, and leading assessments to ensure investments and actions are informed and consistent with the organization's risk environment.

Organizations with a Chief Information Security Officer (CISO) or those that are working toward developing a CISO role, should consider having the CISO and his or her physical security peer both report directly to the CSO. The CISO, in this arrangement, leads the organization's information and data security, including incident response, identity and access management, privacy, and the creation of standards and controls, among others.

Foundational to ERM is conducting and periodically re-evaluating a business or organizational impact analysis. Led by the CSO, this executive effort begins with asking and assessing a few key questions focused on understanding risks that could negatively impact:

- Safe Operations
- Lost Sales and Income Due to Business Disruption

- Brand and Reputational Harm
- Delayed Sales or Income Due to Business Disruption
- Increased Expenses (e.g., overtime labor, outsourcing, expediting costs)
- Regulatory Fines
- Contractual Penalties
- Customer Dissatisfaction or Defection
- Delay of New Business Plans/Investments

To effectively evaluate risk across the organization, the CSO should lead the creation and ongoing work of an executive-level enterprise risk committee, where all aspects of risk are discussed, debated, and defined for the organization. Only when the input from key operations owners is incorporated can an appropriate assessment of risk be made. Periodically convening the risk committee further emphasizes the fact that risk is a whole-of-organization effort.

Ideally, the agency's risk infrastructure will also include some form of proactive risk identification (*i.e.,* external events or trends that could negatively impact the agency or internal vulnerabilities that need to be watched) and documented steps for how the agency will resolve the incident with minimal disruption to service delivery if it occurs. Industry information-sharing groups are an important (and economical) arena for sharing and gathering threat intelligence, security best practices, and vulnerability management insights. As more transit agencies determine what forms of proactive risk identification would be most helpful to their day-to-day operations, they should communicate them directly to their trade associations, the Public Transportation Information Sharing and Analysis Center (PT-ISAC), and other informal groups whose support activities can be tailored to the evolving needs of the group.

Once the risks are understood, an organization can more effectively determine how best to address them. The agency will need to determine if they should accept, reduce, mitigate, avoid, transfer, or control the risk area identified. With this important categorization, an organization can then move towards prioritization, which will shape how they invest in appropriate actions that strengthen the organization's overall resiliency. Coupling a well-developed ERM strategy with industry and regulatory guidance ensures not only compliance but also appropriate investments.

With this new risk baseline established, transit agencies should develop, codify, and document policies for all aspects of the organization's security program. These policies should be designed to ensure consistency in action and should be enforceable as a means of maintaining accountability and oversight. Policies should provide accessible strategies for maintaining security efficacy and clearly define the standards for every individual accountable to each of these policies. Some version of these documents may exist today, though they most likely do not address cyber incidents. If this is the case, agencies should conduct a full review and work to incorporate cyber into each policy and response mechanism.

- **Incident Response and Crisis Management Plans** should ensure the right infrastructure is in place to proactively identify risk indicators that could potentially affect the organization's security posture. This should also include the additional steps that need to be in place to lead the organization through resolving the incident with minimal disruption. The CSO should periodically test the organization's tolerance for risk exposure in key and prioritized areas through tabletop exercises and other means.

- **Resilience Plans** should also include procedures for investing in various areas that minimize disruption. In the cyber domain, it is no longer a question of *if* but *when* an organization will face a ransomware attack. Investing in multiple backups of the organization's sensitive data and/or other security protocols ensures limited downtime when a breach occurs.

- **Communication and Training** are key elements in developing a risk management culture for an organization. Individuals need to be trained and have that training reinforced on a regular basis. Communicating the importance of understanding and being prepared for a variety of risks—whether it be an active shooter or a phishing email—and matching it with appropriate awareness campaigns, exercises, and training will help to create the risk-aware culture that can benefit any organization.

Most Agencies Do Not Have Many of the Basic Policies and Procedures in Place to Respond in the Event of a Cyber Incident[12]

- 42% do not 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

Given the TSA requirement for rail operators to identify a cyber coordinator, all public transit agencies should move towards having a fully integrated 24x7 Security Operations Center (SOC) if and when they are able to do so. The authors acknowledge that this may be impractical or a long way off for many transit operators, but a fully-integrated SOC is a best practice that operators should be aware of. If a SOC is within reach for an agency, appropriate technology and headcount investments should be made to ensure real-time discovery of potential risk indicators and ongoing monitoring of business operations that impact resiliency, investigations, and response. The SOC should include representation from key organizational functions and have access to corollary resources among key vendors that directly support the ERM strategy and benefit from contributing to incident/crisis management. The SOC should also include compliance representation as a role to provide oversight and control to its efforts.

3.3.2 Technology

Once the organization understands its cyber risk exposure, the risk assessment will likely identify key technology needs to reduce relevant risk exposure, standardize processes, and significantly improve how an organization detects, controls, and responds to security risks affecting its operations. Key technology investments include but are not limited to:

- Identity and Access Management
- Network Security
- Data Protection
- Email/web Security
- Endpoint Security
- Asset Management
- Application Security
- Physical Access Control Systems

Specialists exist who focus on providing such services, known as managed security service providers (MSSPs). Larger agencies may have the resources to support some or all of this infrastructure with internal resources; others should augment their team and engage with MSSPs that have experience with and understand the transportation sector and public transit specifically.

A previously identified risk vector for most public transit agencies is the continued use and dependency on legacy and/or unsupported software and hardware. The key is to document and intentionally manage end-of-life (EOL) hardware and software. Only with this documentation does the organization have visibility into the risks EOL infrastructure may pose to the

organization. In addition to making efforts to replace EOL infrastructure in a timely manner, operators should ensure that future implementations do not include firmware or software that is not regularly supported for the entire duration of the life of the system. It is no longer tenable for vendors to exclude at least basic security maintenance from their offerings; agencies should no longer offer RFPs that do not explicitly call out and fund basic security maintenance for the life of the system.

As transit agencies and their vendors work to strengthen their risk management capabilities, the risk management approach of "Security by Design" should be central to how they develop cyber policies and practices. Security by Design is based on the acknowledgment that risk can never be fully avoided and that, instead, the processes by which software is designed, built, and deployed should have built-in layers of security at every step.

11 Security by Design Principles

1. **Defense in Depth:** Also known as layered defense, defense in depth is a security principle where single points of complete compromise are eliminated or mitigated by the incorporation of a series or multiple layers of security safeguards and risk-mitigation countermeasures.

2. **Fail-Safe:** A security principle that aims to maintain confidentiality, integrity and availability by defaulting to a secure state, rapidly recovering software resiliency upon design or implementation failure. In the context of software security, fail-secure is commonly used interchangeably with fail-safe, which comes from physical security terminology.

3. **Least Privilege:** A security principle in which a person or process is given only the minimum level of access rights (privileges) necessary for that person or process to complete an assigned operation. This right must be given only for a minimum amount of time that is necessary to complete the operation.

4. **Separation of Duties:** Also known as the compartmentalization principle, or separation of privilege, separation of duties is a security principle that states that the successful completion of a single task is dependent upon two or more conditions that are insufficient for completing the task by itself.

5. **Economy of Mechanism:** In layman's terms, this is the "Keep It Simple, Stupid" principle because the likelihood of a greater number of vulnerabilities increases with the complexity of the software architectural design and code.

6. **Complete Mediation:** A security principle that ensures that authority is not circumvented in subsequent requests of an object by a subject, by checking for authorization (rights and privileges) upon every request for the object.

7. **Open Design:** The open design security principle states that the implementation details of the design should be independent of the design itself, which can remain open, unlike in the case of security by obscurity, wherein the security of the software is dependent upon the obscuring of the design itself.

8. **Least Common Mechanism:** The security principle of least common mechanisms disallows the sharing of mechanisms that are common to more than one user or process if the users and processes are at different levels of privilege. For example, the use of the same function to retrieve the bonus amount of an exempt employee and a non-exempt employee will not be allowed. In this case the calculation of the bonus is the common mechanism.

9. **Psychological acceptability:** A security principle that aims at maximizing the usage and adoption of the security functionality in the software by ensuring that the security functionality is easy to use and at the same time transparent to the user. Ease of use and transparency are essential requirements for this security principle to be effective.

10. **Weakest Link:** This security principle states that the resiliency of your software against hacker attempts will depend heavily on the protection of its weakest components, be it the code, service, or interface.

11. **Leveraging Existing Components:** This is a security principle that focuses on ensuring that the attack surface is not increased and no new vulnerabilities are introduced by promoting the reuse of existing software components, code, and functionality. [13]

3.3.3 Governance

For agencies to elevate risk management as a priority, so too must the governing bodies that oversee risk for the industry. As the Co-Sector Risk Management Agencies (SRMAs) for the Transportation Sector, the Department of Homeland Security, and the Department of Transportation should prioritize publishing an update to the 2015 Transportation Systems Sector Cybersecurity Framework Implementation Guidance. The vendor community is accelerating their innovation across multiple technologies found commonplace in the sector. The interest and rise of broad CAV adoption are creating new opportunities that enhance operational value while also contributing to increasing the overall risk environment. What was once limited to concern over potentially compromised consumer information and data now also includes the opportunity for a threat actor to exploit cyber vulnerabilities that can control hardware and related autonomous technologies.

The federal agencies should create a Sector Cybersecurity Executive with dedicated investment and authority to establish sector and subsector cybersecurity guidance. The proposed Office of the Cybersecurity Executive (OCE) should model this guidance based on NIST and industry best practices, leveraging a Capability Maturity Model Integration (CMMI) process relevant to the sector. The standard should include prescriptive maturity levels à la the Department of Defense's Cybersecurity Maturity Model Certification (CMMC).[14] The OCE should establish an oversight and inspection capability to conduct periodic assessments and to certify at the established guidance level all transit agencies under their purview, as well as any vendor that maintains (or seeks to develop) an active contractual relationship with an agency.

3.4 An Expanding Regulatory Environment

In a threat environment punctuated by disruptions to critical services resulting from cyber incidents, it should not come as a surprise that regulators are becoming more explicit about cyber risk management expectations for public and private companies alike. Transit operators, regardless of size, provide a critical infrastructure service in the communities in which they operate. The Biden Administration, U.S. Congress, and multiple government agencies are taking steps to sound the alarm for the cyber unaware and taking regulatory actions to encourage—if not mandate—that organizations take steps to improve their cyber resilience.

The Biden Administration has already taken action that is specific to transportation. The TSA on December 2, 2021, issued Security Directive 1582-21-01: "Enhancing Public Transportation and Passenger Railroad Cybersecurity" (the Security Directive) for each owner/operator of a passenger railroad carrier or rail transit system.[15] APTA believes that the Security Directive applies to approximately 23 rail transit systems.[16] This Security Directive was issued simultaneously with a similar Information Circular Surface Transportation IC-2021-01 for all surface transportation owners/operators, whereby TSA "recommends" that they too follow the same directives.[17] Though not yet compulsory, it is expected that the TSA will eventually convert this

recommendation into a formal security directive. The remaining critical infrastructure sectors should expect similar mandates.

The Security Directive requires the owner/operator of an applicable passenger railroad carrier or rail transit system to:

- Designate a Cybersecurity Coordinator who is required to be available to TSA and CISA 24/7 to coordinate cyber practices and address any incidents;
- Report cybersecurity incidents to CISA no later than 24 hours after a cybersecurity incident is identified;
- Develop and adopt a Cybersecurity Incident Response Plan; and
- Conduct a cybersecurity vulnerability assessment using a form provided by TSA.[18]

An owner/operator must immediately notify TSA if it is unable to implement any of the measures in the Security Directive and may provide a proposed alternative measure for TSA approval.

How vendors will be expected to support this and future directives is not yet defined, though the authors expect that key transit vendors will, at a minimum, be required to mirror the above requirements when providing critical services to public transit agencies. Vendors and agencies should expect the regulatory regime governing cybersecurity to become more precise as more resources are directed to addressing the growing global cyber threat.

The Biden Administration, since taking office in January 2021, has been a vocal supporter of the need for greater engagement in cybersecurity by the Federal Government. Spurred in part by headline grabbing hacks that have hobbled everything from U.S. fuel pipelines to healthcare systems, there is bipartisan support for efforts to strengthen the cyber posture of the U.S. public and private sectors.

President Biden on May 12, 2021, issued Executive Order – 14028, marking the start of a growing bevvy of regulatory guidance coming from the White House on cyber-related matters. The Executive Order (EO) applies specifically to federal agencies and their suppliers.

> It is the policy of my Administration that the prevention, detection, assessment, and remediation of cyber incidents is a top priority and essential to national and economic security. The Federal Government must lead by example. All Federal Information Systems should meet or exceed the standards and requirements for cybersecurity set forth in and issued pursuant to this order.[19]

The U.S. DOT is taking further steps to support improved cyber practices and serve its constituents. It has updated website materials to reflect the most current internal and external

guidance on managing cyber risks, is providing much needed funding to state and local transportation agencies that have struggled to fund cybersecurity activity, and is funding research in all modes to identify ways to make agencies more cyber resilient.[20]

The FTA has also added cybersecurity as part of the Triennial Review of grantees and is in the process of developing cybersecurity expectations for grantees that the FTA can assess. It is not unreasonable to assume that the FTA expectation will align with the requirements outlined in the Security Directive[21]

In addition to the steps taken by the Biden Administration to strengthen the cyber capabilities of the U.S. defense and intelligence systems, the Office of Management and Budget, on January 26, 2022, released a memo to the heads of all executive departments and agencies outlining the U.S. Government's move toward "zero trust" cybersecurity principles.[22]

> "The foundational tenet of the Zero Trust Model is that no actor, system, network, or service operating outside or within the security perimeter is to be trusted. Instead, we must verify anything and everything attempting to establish access. It is a dramatic paradigm shift in philosophy of how we secure our infrastructure, networks, and data, from verify once at the perimeter to continual verification of each user, device, and application, and transaction."

The detailed memo instructs Federal agencies and offices on how the government intends to implement EO 14028 and the specific standards and objectives that need to be in place by the end of Fiscal Year 2024. The memo specifically cites contractors and partners (*i.e.*, individuals or organizations external to the agency but with access to the agency system) as needing to comply with security protocols such as the use of multi-factor authentication. As agencies work to implement more of these practices into their own operations, the authors expect that more will be required of vendors.

3.4.1 Other Regulatory Activity

In addition to the above, the following activity around cyber risk management is occurring that may (eventually) effect the public transit vendor ecosystem:

U.S. Department of Defense (DOD)

The Department of Defense in November 2020 began using the Cybersecurity Maturity Model Certification (CMMC), which is a unifying standard for vendors to ensure they implement cybersecurity across the Defense Industrial Base (DIB).

The CMMC program includes cyber protection standards for companies in the defense industrial base (DIB). By incorporating cybersecurity standards into acquisition programs, CMMC provides the Department assurance that contractors and subcontractors are meeting DoD's cybersecurity

requirements. The DIB is the target of increasingly frequent and complex cyberattacks by adversaries and non-state actors. Dynamically enhancing DIB cybersecurity to meet these evolving threats, and safeguarding the information that supports and enables our warfighters, is a top priority for the Department. CMMC is a key component of the Department's expansive DIB cybersecurity effort.[23]

Again, the CMMC currently applies only to contractors in the DIB; however, procurement practices that start in the defense arena regularly move into the non-defense arena, and procurement and cybersecurity professionals both anticipate this transition.

United States Congress

Congress has also been very active in regulating cybersecurity over the past year. In addition to the multitude of bills making their way through Congress, Congress passed several pieces of legislation in 2021 having significant cybersecurity implications for the transit industry.

One important piece of legislation is the Infrastructure Investment and Jobs Act (IIJA), passed by Congress in November 2021, investing over $1 trillion of federal money to strengthen the nation's infrastructure and fund other key programs and initiatives.[24] Because cybersecurity is viewed as one of the most vulnerable and critical components of the nation's infrastructure, cybersecurity funding, enhancement, and maturity are woven throughout the bill. The IIJA provides new "maturity models" that standardize cybersecurity policies and practices. The Act also provides assistance for businesses, state and local governments, and other entities to prepare for and protect against cyberattacks.

The bill allocates approximately $2 billion to strengthen the nation's cyber defenses. The IIJA's notable cybersecurity appropriations include:

- $1 billion for grants to improve state and local government cybersecurity;
- $250 million to fund the Rural and Municipal Utility Advanced Cybersecurity Grant and Technical Assistance Program—a program designed to support public utilities and other eligible entities;
- $250 million to develop "advanced cybersecurity applications and technologies for the energy sector";
- $20 million per year for fiscal year 2022, and every year thereafter until 2028, to create a Cyber Response and Recovery Fund to help public and private entities respond to a significant cyber incident;

- $158 million for the US Department of Homeland Security's Science and Technology Directorate to fund "critical infrastructure security and resilience research, development, test, and evaluation";

- $35 million to CISA for "risk management operations and stakeholder engagement and requirements"; and

- $21 million to fund the recently created Office of the National Cyber Director (ONCD).

Another significant piece of legislation impacting transportation is the National Defense Authorization Act (NDAA) for the Fiscal Year 2022.[25] The NDAA includes several important public transportation provisions, including specifics on cybersecurity and transit security grants.[26] For example, the NDAA:

- Requires the Director of the CISA to establish a program, to be known as "CyberSentry", to provide continuous monitoring and detection of cybersecurity risks to critical infrastructure entities that own or operate industrial control systems (ICS) that support national critical functions, upon request and subject to the consent of the owner or operator. Under a CyberSentry partnership agreement, CyberSentry will provide technical assistance, such as continuous monitoring of ICS and the information systems that support such systems, detection of cybersecurity risk to such ICS, and other cybersecurity services as agreed upon;[27]

- Requires the Secretary of DHS to prioritize the assignment of TSA and DHS officers and intelligence analysts to locations with participating state, local, and regional fusion centers in jurisdictions with high-risk surface transportation assets to enhance the security of such assets, including by providing timely information sharing regarding threats of terrorism, targeted violence, and other threats. Under the provision, the DHS Secretary is required to make security clearances available to appropriate owners and operators of surface transportation assets to foster greater sharing of classified information relating to threats of terrorism, and other threats to surface transportation assets;[28]

- Expands the operating use of funds for the public transportation security assistance grant program to include "associated backfill" (*e.g.,* backfilling personnel attending an approved training course or program);[29] and

- Requires the Government Accountability Office to conduct a review of the public transportation security assistance program and report to Congress no later than one year after the date of enactment of this Act, and again no later than five years after enactment.[30]

One of the requirements that came out of FY 2021 NDAA was to implement a CSC recommendation that CISA establish a Cybersecurity Advisory Committee (CSAC).[31] The CSAC was established in June 2021 and named the first 23 of the 35 members in December 2021.

The CSAC is directed to establish subcommittees for information exchange, critical infrastructure, risk management, and public and private partnerships. The members, who include representatives from industry, government technology, and security leaders, will advise the CISA Director on the agency's policies and programs.

On March 15, 2022, President Biden signed into law the omnibus spending law which, in part, covered entities to report cyber incidents and ransom payments. The relevant portion of this law, titled the Cyber Incident Report for Critical Infrastructure Act of 2022 proposes reporting requirements for incidents, establishes new programs to curtail ransomware attacks and encourages information sharing between government agencies.[32]

Opportunities for vendors to leverage this regulatory activity to better support their public transit clients and to differentiate themselves in the industry through the maturity of their security practices are expanding and accelerating. Vendors that can help their current and future clients anticipate and comply with regulatory guidance and mandates are likely to find their services in high demand.

4. Recommendations

The authors of this report believe there are several steps transit agencies and their vendor community can take to strengthen their collective cybersecurity posture, all while maintaining a state of operational resilience and readiness. These measures require executive focus and investment across the transit ecosystem. This includes the need for a robust regulatory environment explicitly enforced by the appropriate U.S. government agencies and departments overseeing their critical infrastructure sector. Consistent with DHS's Transportation Systems Sector Cybersecurity Framework Implementation Guidance [33] and NIST Framework for Improving Critical Infrastructure Cybersecurity,[34] the following recommendations are provided.

Vendors

- Vendors for critical systems should make available a security lead to assist the agency CSO in the management of the agency's risk.

- Vendors should establish a cadence for periodic and independent security audits and penetration testing of their own environments. The results should be provided to their agency clients along with a mutually acceptable and binding commitment to a set of actions and timeframes necessary to mitigate any identified risks.

- Vendors should engage in existing public-private security information sharing forums and codify procedures for how relevant data is submitted to and from all member organizations for common benefit. Key among these groups are:

    - APTA's Control Communications Security Working Group (CCSWG)

    - APTA's Enterprise Cybersecurity Working Group (ECSWG)

    - Surface and Public Transportation ISAC

Transit Agencies

- Transit agencies should integrate their cyber risk management program with their existing physical security risk management organization and infrastructure, creating a holistic ERM program.

    - Evaluations of existing plans should be discussed and approved by the agency's enterprise risk committee.

    - Transit agency security policies should be updated to include existing standards, activities, requirements, and other elements introduced by combining physical and cyber risk management.

- Existing security training should be augmented with cybersecurity training for all agency personnel.

- Transit agencies should elevate security within the organization by appointing a CSO who has the authority, investment, and responsibility for both existing physical security operations, as well as the information and cyber security domains.

- An executive-level enterprise risk committee, chaired by the CSO, should be established that includes, at a minimum, the chief financial officer, chief legal officer, and the head of operations.

- Transit agencies should engage in existing public-private security information sharing forums and codify procedures for how relevant data is submitted to and from all member organizations for common benefit. Key among these groups are:

    - APTA's Control Communications Security Working Group (CCSWG)

    - APTA's Enterprise Cybersecurity Working Group (ECSWG)

    - Surface and Public Transportation ISAC

- Transit agencies should immediately identify and evaluate all software and hardware that is EOL with no opportunity for updates or security patches. If such technologies are identified, every attempt should be made to reduce and/or eliminate reliance on them with a plan in place to acquire an appropriate replacement.

Associations

- APTA, working with other stakeholders, should develop third-party risk management and oversight standards. Given the nature of the dependencies across the supply chain between transit operators and their vendors, it is vital that this standards development effort include the participation of professionals from disciplines such as procurement, physical security, cybersecurity, and legal.

- APTA and other industry support organizations should integrate the third-party risk management and oversight standards into templates for contract language, RFPs, and other artifacts that operators can rely on to engage the vendor community.

- APTA, working with its stakeholders, should develop a comprehensive security questionnaire and assessment guide that transit operators can have vendors complete prior to submitting a proposal. This questionnaire should be based on regulatory guidance and, in its absence, should follow standards outlined by the NIST Risk Management Framework and Cybersecurity Framework.

- APTA, working with other stakeholders, should create minimum guidelines for cybersecurity audits, penetration tests, and other tools to understand enterprise risk in the public transit environment.

- APTA, working with other stakeholders, should provide guidance on the size and scope of investments that operators should make in risk management to operationalize all aspects of their security program, including managing cyber risk.

U.S. Government

DHS and U.S. DOT should create a Sector Cybersecurity Executive with dedicated investment and authority to establish sector and subsector cybersecurity guidance.

- DHS and U.S. DOT should prioritize updating the 2015 Transportation Systems Sector Cybersecurity Framework Implementation Guidance to reflect the advent of CAVs.

- The FTA should require all procurements using federal dollars to include and fund basic security maintenance when software and firmware are procured.

- The FTA should require that all transit agencies meet the basic requirements set forth in TSA Security Directive 1582-21-01: "Enhancing Public Transportation and Passenger Railroad Cybersecurity for Passenger Rail."

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

- The FTA should create an attestation program whereby transit CEOs are required to attest that their organization has completed an annual cybersecurity audit prior to receiving funding.

- Congress should increase funding to DHS and the U.S. DOT to develop and promulgate a set of minimal cybersecurity standards and tools 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 the U.S. DOT and DHS work together to improve cybersecurity preparedness within the TSS.

5. Conclusion

Building a cyber-risk aware culture in public transit will take time and require resources as operators work to design and integrate comprehensive risk management strategies. Doing so in a timely and effective manner will require that each of the stakeholders identified in this report—transit agencies, vendors, associations, and government—do their part in support of maturing the industry's cyber capabilities.

In the last few years, cyber-attacks on transportation have increased, and transit agencies, along with every other sector of the economy have become a target for nefarious actors seeking to disrupt operations, be it for personal or political gain. The avenues to exploit this vital infrastructure will continue to evolve along with the technology that enables the industry to meet its core operations and customer demands. As these technologies are further embedded in operations, new vulnerabilities will arise, and organizations need to be prepared to adapt and respond. With expanded and focused risk management strategies, continuing education, and a willingness to evolve with the threat environment, public transit agencies have the ability to institute policies and practices that will continue their positive record of delivering services with safety and quality. Accounting for risk today will foster greater resiliency and preparedness for tomorrow.

Appendix A: Literature Review and Available Support

Both the public and private sectors have developed a great deal of cybersecurity guidance over the past two decades. Cybersecurity experts will tell you that the tools used to manage cybersecurity and associated threats do not vary greatly across industries, but that some industries are more mature in their understanding when it comes to managing cyber risks. Industries such as the financial management industry, where billions of dollars are moved digitally every minute, have been forced to invest heavily in cybersecurity protection. Other industries, such as the transit industry, which has traditionally been a hardware-based industry relying largely on firmware and closed networks, have not faced the same urgency until recently.

The 2020 Report observes that "[t]he existing cybersecurity guidance for public transit is spread across numerous government and industry entities. . . [and that] federal resources exist for agencies to improve their cybersecurity readiness."[35] The same baseline documents are at the core of every industry cybersecurity program. Despite industry differences, cybersecurity maturity models and the assessment practices used to strengthen policies, procedures, and practices are transferable.

One of the key foundations of cybersecurity programs across any industry comes from the National Institute of Standards and Technology (NIST). NIST is a non-regulatory agency that has no authority to dictate the use of any standard, but its standards carry significant weight. The work of NIST is defined by federal statutes, executive orders, and policies—including developing cybersecurity standards and guidelines for federal agencies. NIST's cybersecurity program supports its overall mission to promote U.S. innovation and industrial competitiveness by advancing measurement science, standards, and related technology through research and development.[36]

NIST in 2014 released the "Framework for Improving Critical Infrastructure Security" in response to Presidential Executive Order 13636, *Improving Critical Infrastructure Cybersecurity*,[37] which called for a standardized security framework for critical infrastructure in the United States. This guidance is not intended to be 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. The guidance is equally applicable to public and private industry.

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.[38]

To further support organizations in the face of a growing cyber threat, Congress established the Cybersecurity Information Security Agency (CISA) at the U.S. Department of Homeland Security (DHS) through the Cybersecurity and Infrastructure Security Agency Act of 2018.[39] According to DHS, "CISA is the Nation's risk advisor, working with partners to defend against today's threats and collaborating to build more secure and resilient infrastructure for the future."[40] CISA coordinates a collective defense to identify and vet procedures to manage and reduce the impact of disruption to critical infrastructure. In this role, the organization builds and coordinates relationships across industries working with sector-specific agencies, such as the U.S. DOT, the FTA, and the TSA, among others.

CISA's role is to unite government and private sector partners, with a particular focus on 16 Critical Infrastructure Sectors:

> 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, national public health or safety, or any combination thereof.[41]

The public transit industry is part of the Transportation Security Sector (TSS), which is one of the 16 critical sectors. As such, the industry has direct access to CISA's capabilities and resources, such as intelligence analysis, data assessment, response methods development, and assistance to manage risks to critical infrastructure that often spike from emerging threats. CISA leads a systematic approach to manage and reduce cyber risk that includes providing services, cyber training, support to critical infrastructure operators, and risk analysis.

The TSA, also housed within DHS, is another critical cybersecurity actor within the Federal government. 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."[42] 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, -- both physical and cyber."[43] 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.[44]

DHS in 2015 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."[45] 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.[46] The TSS Cybersecurity Framework Implementation Guidance and its companion workbook provide an approach for Transportation Systems Sector[47] owners and operators to apply the tenets of the National Institute of Standards and Technology Cybersecurity Framework to help reduce cyber risks.

Appendix B: Email Request to Potential Survey Participants

Good Afternoon

As you know cybersecurity issues are top of mind for us all these days. We have seen major national attacks with SolarWinds, Microsoft, Colonial Pipeline, and Kaseya. The transit industry has also experienced a number of high-profile attacks on MTA, Martha's Vineyard Ferry, SEPTA, and Vancouver. Last year the Mineta Transportation Institute (MTI) released an important study that should have been a wakeup call for us all Is the Transit Industry Prepared for the Cyber Revolution? Policy Recommendation to Enhance Surface Transit Cyber Preparedness. After surveying more than a third of American Public Transportation Association's (APTA) public transit members, the researchers concluded that the industry was ill prepared for the developing cyber threat. The study was very helpful in identifying several recommendations for the Federal Transit Administration, APTA, and public transit operators, many of which are being implemented and are starting to make a difference.

MTI has engaged the same researchers to look at the relationship between the public transit operators and their vendors to identify how together they can better secure their cybersecurity posture. The researchers immediately reached out to APTA and its Business Members Board of Governors to engage their support. We have met several times over the past few months as the researchers developed a report outline, survey guide and interview list. Their intent is to interview a representative sample of public transit operators and vendors to better understand how they currently work together to manage their cybersecurity exposure and what they can do to make improvements.

The purpose of this study is to highlight best practices and to identify resources and tools that we all should be taking advantage of going forward. We are all engaged in some level of cybersecurity protection, but can all afford to do more. Only by working together - agencies and vendors - can we effectively mature our industry's posture against cyber threats. Moreover, this Administration has placed a priority on cybersecurity, with new requirements and regulations on the horizon. To the extent that we can get ahead of the curve, the better off we will be.

We recommend that you participate in this study. Clever Devices did and it was worth our time as we learned alongside the researchers. Your organization can choose to participate anonymously on not, it is up to you. The initial interview will take about an hour and there may be some follow-up depending on how the initial interview goes.

Attached you will find an abstract of the study as well as a copy of the survey questions so that you can make sure that you have the correct individual or individuals available for the interview. Scott Belcher, the MTI Research Associate, will follow-up with you to answer any questions and to schedule an interview.

Best regards,

Buddy Coleman
Chief Customer Officer
Clever Devices
Vice Chair, APTA, BMBG

Polly Hanson
Senior Director of Security, Risk and Emergency Management
American Public Transit Association

Scott Belcher
Research Associate
Mineta Transportation Institute

Appendix C: Interview Guide

Date

Name:

Job Title: Organization:

Email: Phone:

Core Questions

Tell me about your company—What services do you offer? Who are your customers?

Which of these services do you provide to your transit industry customers? How?

Tell me about how you view the cyber risk landscape for the U.S. transit industry

Who manages the cyber relationship with you—the vendor—from within the transit provider? What about from your organization?

What does interaction with your transit client(s) look like? Are you meeting regularly? Providing risk assessments on a scheduled basis? Only connecting when there's an issue? Is it documented?

Have your transit clients established specific cyber responsibilities/expectations from you with respect to your operations? With respect to your provision of services? If so, how? Do you have a service level agreement in place?

What sets you apart from other vendors serving transit clients?

The transit industry is behind in incorporating cybersecurity into enterprise risk management practices—what are you doing to help your clients with this?

Company/Service Details

Do you have a cybersecurity program in place? If not formal, please describe activities engaged to secure your systems.

If a formal program is in place, please describe your operations by category:

Security Operations

Tell me about your general approach to threat detection, incident response, and recovery within your own company. As it relates to your transit clients.

Security Architecture

Tell me about your company's approach to network security architecture—core components, frequency of risk evaluations, special considerations for the transit industry

Governance

What, if any, requirements coming from outside your organization govern the services you provide to your clients?

What kind of guidance or interface do you have with local, state, or federal government regarding cybersecurity in general or your services more specifically?

What kind of processes, procedures, and controls do you have in place to ensure compliance and execution of your cybersecurity program? Are your clients involved? If so, how so?

User Education

Do you offer your staff training in information and network security to improve their baseline of understanding? What about your clients?

Threat Intelligence

How do you monitor threats to your own organization? Your clients? Proprietary network? Third-party threat tools?

Risk Assessment

What does your company's risk assessment process entail? How frequently do you provide this to your clients?

Risk Management

What does the delivery of risk management services look like for the transit industry? (i.e., risk appetite for a public-serving organization, resiliency, and business continuity)

NOTE// Vendor Interview Guide: The goal of the vendor interview is to gain a better understanding about the services delivered to transit providers, the sophistication of such services—specifically as pertains to the identification, prevention, and response to infosec risks—

and the driving force behind the quality of these services. The objective is to find a few good examples of vendors doing cybersecurity right. Secondary goal is to induce vendor to take a closer look at their cybersecurity practices, and to seed the idea that good cybersecurity hygiene can be a competitive advantage.

Endnotes

[1] Scott Belcher, Terri Belcher, Eric Greenwald, Brandon Thomas, *Is the Transit Industry Prepared for the Cyber Revolution? Policy Recommendations to Enhance Surface Transit Cyber Preparedness*. Mineta Transportation Institute, September 2020. DOI 10.31979/mti.2020.1939 https://transweb.sjsu.edu/sites/default/files/1939-Belcher-Transit-Industry-Cyber-Preparedness.pdf (accessed January 5, 2022).

[2] Ibid.

[3] These are the "Five Functions" that act as the backbone for the Cybersecurity Framework established by the National Institute of Standards and Technology May 12, 2021. https://www.nist.gov/cyberframework/online-learning/five-functions (accessed February 8, 2022).

[4] Checkpoint "Ransomware Attacks Continue to Surge, Hitting a 93% Increase Year Over Year" https://blog.checkpoint.com/2021/06/14/ransomware-attacks-continue-to-surge-hitting-a-93-increase-year-over-year/ (accessed February 1, 2022).

[5] Accenture. "All Aboard! How Hackers Are Moving in on the Transit Sector" June 22, 2020. .https://www.accenture.com/us-en/blogs/cyber-defense/hackers-moving-in-on-transit-sector (accessed March 1, 2022).

[6] APTA, 2021 Public Transportation Fact Book, May 2021, 16 https://www.apta.com/wp-content/uploads/APTA-2021-Fact-Book.pdf (accessed March 3, 2022).

[7] APTA, 2021 Public Transportation Fact Book, May 2021, 16 https://www.apta.com/wp-content/uploads/APTA-2021-Fact-Book.pdf (accessed March 3, 2022).

[8] APTA, 2021 Public Transportation Fact Book, May 2021, 27 https://www.apta.com/wp-content/uploads/APTA-2021-Fact-Book.pdf (accessed March 3, 2022).

11 APTA, 2021 Public Transportation Fact Book, May 2021, 27 https://www.apta.com/wp-content/uploads/APTA-2021-Fact-Book.pdf (accessed March 3, 2022).

[10] National Academies of Sciences, Engineering, and Medicine 2022. Cybersecurity in Transit Systems. Washington, DC: 2022 The National Academies Press.32 https://doi.org/10.17226/26475 (accessed February 10, 2022).

[11] CISA. "Cybersecurity and Physical Security Convergence." https://www.cisa.gov/sites/default/files/publications/Cybersecurity%20and%20Physical%20Security%20Convergence_508_01.05.2021_0.pdf (accessed March 10, 2022).

[12] Scott Belcher, Terri Belcher, Eric Greenwald, Brandon Thomas, *Is the Transit Industry Prepared for the Cyber Revolution? Policy Recommendations to Enhance Surface Transit Cyber Preparedness*. Mineta Transportation Institute, September 2020. https://transweb.sjsu.edu/sites/default/files/1939-Belcher-Transit-Industry-Cyber-Preparedness.pdf

[13] GITHUB "01-Principles of Security Engineering.md" https://github.com/OWASP/DevGuide/blob/master/02-Design/01-Principles%20of%20Security%20Engineering.md (accessed February 8, 2022).

[14] Office of the Undersecretary of Defense – Acquisition & Sustainment. "Securing the Defense Industrial Base CMMC 2.0." https://www.acq.osd.mil/cmmc/ (accessed February 8, 2020).

[15] Department of Homeland Security. Security Directive 1582-21-01 "Enhancing Public Transportation and Passenger Railroad Cybersecurity." December 2, 2021. https://www.tsa.gov/sites/default/files/sd-1582-21-01_signed.pdf (accessed February 9, 2022).

[16] APTA "APTA Appendix TSA-Security Directive 1582-21-"Applicable Public Transportation and Passenger Railroads." December 8, 2021. https://www.apta.com/wp-content/uploads/APTA-APPENDIX-TSA-Security-Directive-1582-21-01-12.08.2021.pdf (accessed February 9, 2022).

[17] Department of Homeland Security. Information Circular: "Surface Transportation IC-2021-01: Enhancing Surface Transportation Cybersecurity." December 31, 2021. https://www.tsa.gov/sites/default/files/20211201_surface-ic-2021-01.pdf (accessed February 9, 2022).

[18] TSA. Security Directive 1582-21-01. "Enhancing Public Transportation and Passenger Railroad Cybersecurity. December 31, 2021. https://www.tsa.gov/sites/default/files/sd-1582-21-01_signed.pdf.

[19] Joseph R. Biden, Executive Order 14028 (2021) Improving the Nation's Cybersecurity. 86 FR26633 https://www.federalregister.gov/documents/2021/05/17/2021-10460/improving-the-nations-cybersecurity.

[20] Federal Transit Administration. "Cybersecurity Resources for Transit Agencies." https://www.transit.dot.gov/regulations-and-programs/safety/cybersecurity-resources-transit-agencies (accessed May 16, 2022)

[21] Federal Transit Administration. "Triennial Reviews." January 27, 2022. https://www.transit.dot.gov/funding/grantee-resources/triennial-reviews/triennial-reviews (accessed May 16, 2022)

[22] Office of Management and Budget. "Memorandum For The Heads of Executive Departments and Agencies: Moving the U.S. Government Toward Zero Trust Cybersecurity Principles. January 26, 2022. https://www.whitehouse.gov/wp-content/uploads/2022/01/M-22-09.pdf (accessed March 10, 2022).

[23] Department of Defense. "Strategic Directions for Cybersecurity Maturity Model (CMMC) Program, November 4, 2021 https://www.defense.gov/News/Releases/Release/Article/2833006/strategic-direction-for-cybersecurity-maturity-model-certification-cmmc-program/ (accessed March 11, 2022).

[24] U.S. Congress. Public Law 117-58. November 15, 2021. https://www.congress.gov/117/plaws/publ58/PLAW-117publ58.pdf (accessed February 24, 2022).

[25] The White House. "Statement by the President on S. 1605, the National Defense Authorization Act of Fiscal Year 2022." December 27, 2021. https://www.whitehouse.gov/briefing-room/statements-releases/2021/12/27/statement-by-the-president-on-s-1605-the-national-defense-authorization-act-for-fiscal-year-2022/ (accessed March 2, 2022).

[26] Many of the requirements in the NDAA come from the recommendations of the Cyberspace Solarium

Commission (CSC) which was established in the FY 2019 NDAA and expired at the end of FY 2021. 26 of its recommendations and 50 cyber provisions were included in the FY 2022 NDAA. It was the first time so many cyber provisions made it into the annual defense bill. The CSC will become "Solarium 2.0," a non-profit organization that will continue to advance cybersecurity issues through Congress while also exploring new territory, such as recovering ransom funds.

[27] U.S. Congress. Public Law 117-58. Section 1548. November 15, 2021. https://www.congress.gov/117/plaws/publ58/PLAW-117publ58.pdf (accessed February 24, 2022).

[28] U.S. Congress. Public Law 117-58. November 15, 2021. Section 6418 https://www.congress.gov/117/plaws/publ58/PLAW-117publ58.pdf (accessed February 24, 2022).

[29] U.S. Congress. Public Law 117-58. Section 6420 November 15, 2021. https://www.congress.gov/117/plaws/publ58/PLAW-117publ58.pdf (accessed February 24, 2022).

[30] U.S. Congress. Public Law 117-58. Section 6422 November 15, 2021. https://www.congress.gov/117/plaws/publ58/PLAW-117publ58.pdf (accessed February 24, 2022).

[31] CISA "CISA Cybersecurity Advisory Committee. Updated February 1, 2022 https://www.cisa.gov/cisa-cybersecurity-advisory-committee (accessed February 18, 2022).

[32] United States House of Representatives H.R 2471 – Consolidated Appropriations Act, 2022 Cyber Incident Reporting for Critical Infrastructure Act of 2022, March 15, 2022 H.R. 2471, 116th Cong. (2022).

[33] 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 (accessed February 18, 2022).

[34] National Institute of Standards and Technology (NIST) Framework for Improving Critical Infrastructure. Cybersecurity April 16, 2018, https://nvlpubs.nist.gov/nistpubs/cswp/nist.cswp.04162018.pdf (accessed February 18, 2022).

[35] Scott Belcher, Terri Belcher, Eric Greenwald, Brandon Thomas, Is the Transit Industry Prepared for the Cyber Revolution? Policy Recommendations to Enhance Surface Transit Cyber Preparedness. Mineta Transportation Institute, September 2020. 35 DOI 10.31979/mti.2020.1939 https://transweb.sjsu.edu/sites/default/files/1939-Belcher-Transit-Industry-Cyber-Preparedness.pdf (accessed January 5, 2022).

[36] National Institute of Standards and Technology (NIST) "Cybersecurity" https://www.nist.gov/cybersecurity accessed March 1, 2022).

[37] 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.

[38] National Institute of Standards and Technology (NIST), "Framework for Improving Critical Infrastructure Cybersecurity," April 16, 2018, https://nvlpubs.nist.gov/nistpubs/CSWP/NIST.CSWP.04162018.pdf (accessed February 24, 2022).

[39]United States House of Representatives H.R.3359 Cybersecurity and Infrastructure Security Agency Act of 2018 November 16, 2018, https://www.congress.gov/bill/115th-congress/house-bill/3359 (accessed March 3, 2022).

[40] Cybersecurity and Infrastructure Security Agency (CISA) "About CISA" https://www.cisa.gov/about-cisa (accessed March 1,2022).

[41] Cybersecurity and Infrastructure Security Agency (CISA) "Critical Infrastructure Sectors." https://www.cisa.gov/critical-infrastructure-sectors (accessed March 1, 2022).

[42] Transportation Security Administration (TSA), "Mission," https://www.tsa.gov/about/tsa-mission (accessed March 1, 2022).

[43] TSA, "TSA Releases Cybersecurity Roadmap," December 4, 2018, https://www.tsa.gov/news/releases/2018/12/04/tsa-releases-cybersecurity-roadmap (accessed March 1, 2022).

[44] TSA, "Cybersecurity Roadmap 2018," 4 November 2018, https://www.tsa.gov/sites/default/files/documents/tsa_cybersecurity_roadmap.pdf (accessed March 1, 2022).

[45] 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 18, 2022).

[46] Department of Homeland Security, 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 18, 2022).

[47] CISA, "Transportation Systems Sector," https://www.cisa.gov/transportation-systemssector (accessed March 7, 2022).

Abbreviations and Acronyms

AASHTO	American Association of State Highway Transportation Officials
APTA	American Public Transit Association
AVL	Automatic Vehicle Locator
BMBG	Business Members Board of Governors (APTA)
CAV	Connected and Automated Vehicles
CCSWG	Control Communications Security Working Group (APTA)
CISA	Cybersecurity and Infrastructure Security Agency
CISO	Chief Information Security Officer
CMMC	Cybersecurity Maturity Model Certification
CMMI	Capability Maturity Model Integration
COSO	Committee of Sponsoring Organizations
CRO	Chief Risk Officer
CSC	Cyberspace Solarium Commission
CSAC	Cybersecurity Advisory Committee
CSO	Chief Security Officer
CTO	Chief Technology Officer
DIB	Defense Industrial Base
DHS	United States Department of Homeland Security
DoD	United States Department of Defense
DOT	United States Department of Transportation
ECSWG	Enterprise Cybersecurity Working Group (APTA)

EO	Executive Order
EOL	End-of-Life
ERM	Enterprise Risk Management
FedRAMP	Federal Risk and Authorization Management Program
FTA	Federal Transit Administration
GAO	Government Accounting Office
GPS	Global Positioning Systems
ICS	Industrial Control Systems
ICT	Information Communications Technology
IIJA	Infrastructure Investment and Jobs Act
ISO	International Organization for Standardization
IT	Information Technology
ITS	Intelligent Transportation Systems
MSSP	Managed Security Service Providers
MTA	Metropolitan Transportation Authority
MTI	Mineta Transportation Institute
NCF	National Critical Functions
NDAA	National Defense Authorization Act
NIST	National Institute of Standards and Technology
OCE	Office of the Cybersecurity Executive
OMB	Office of Management and Budget
ONCD	Office of the National Cyber Director
OT	Operational Technology

PCI	Payment Card Industry
PII	Personally Identifiable Information
PT-ISAC	Public Transportation Information Sharing and Analysis Center
RFP	Request for Proposal
SEPTA	Southeastern Philadelphia Transportation Authority
SOC	Security Operations Center
SCRM	Supply Chain Risk Management
SRMA	Sector Risk Management Agencies
TRB	Transportation Research Board
TSA	Transportation Security Agency
TSS	Transportation Security Sector

Bibliography

Accenture. "All Aboard! Hackers Moving in on Transit Sector." June 22, 2020. https://www.accenture.com/us-en/blogs/cyber-defense/hackers-moving-in-on-transit-sector (accessed March 1, 2022)

American Public Transportation Association (APTA). 2021 Public Transportation Fact Book. May 2021. https://www.apta.com/wp-content/uploads/APTA-2021-Fact-Book.pdf (accessed March 3, 2022).

American Public Transportation Association (APTA) Security Risk Assessment Methodology for Public Transit, March 23, 2021. https://www.apta.com/wp-content/uploads/APTA-SS-SIS-S-017-21.pdf (accessed March 3, 2022).

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 February 28, 2022).

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 February 28, 2022).

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 February 28, 2022).

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 February 28, 2022).

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 February 28, 2022).

American Public Transportation Association (APTA). Recommended Practice "SecuringControl 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 February 28, 2022).

APTA "APTA Appendix TSA-Security Directive 1582-21-"Applicable Public Transportation and Passenger Railroads." December 8, 2021. https://www.apta.com/wp-content/uploads/APTA-APPENDIX-TSA-Security-Directive-1582-21-01-12.08.2021.pdf (accessed February 9, 2022).

Barker, William, Karen Scarfone, William Fisher, Murugiah Souppaya"Cybersecurity *Framework Profile for Ransomware Risk Management*, National Institute of Standards and Technology September 2021. https://doi.org/10.6028/NIST.IR.8374-draft.(accessed March 16, 2022).

Belcher, Scott, Terri Belcher, Eric Greenwald, Brandon Thomas. *Is the Transit Industry Prepared for the Cyber Revolution? Policy Recommendations to Enhance Surface Transit Cyber Preparedness.* San Jose State University – Mineta Transportation Institute.September 2020, DOI 10.31979/mti.2020.1939 https://transweb.sjsu.edu/sites/default/files/1939-Belcher-Transit-Industry-Cyber-Preparedness.pdf (accessed January 5, 2022).

Biden, Joseph R. Executive Order-14028. Improving the Nation's Cybersecurity. *86 FR26633*. May 17, 2021.

Biden, Joseph R. Executive Order-14017. America's Supply Chains. *86 FR11849*. March 1, 2021.

Checkpoint. "Ransomware Attacks Continue to Surge, Hitting a 93% Increase Year Over Year." https://blog.checkpoint.com/2021/06/14/ransomware-attacks-continue-to-surge-hitting-a-93-increase-year-over-year/ (accessed February 1, 2022).

Committee of Sponsoring Organizations of the Treadway Commission (COSO). *Enterprise Risk Management Integrated Framework Executive Summary*. September 2004. 2, https://www.coso.org/documents/coso-erm-executive-summary.pdf (accessed February 8, 2022).

Cybersecurity and Infrastructure Security Agency (CISA). "Critical Infrastructure Sectors." https://www.dhs.gov/cisa/critical-infrastructure-sectors (accessed March 1, 2022).

Cybersecurity and Infrastructure Security Agency (CISA). "About CISA." https://www.cisa.gov/about-cisa (accessed March 1, 2022).

Cybersecurity and Infrastructure Security Agency (CISA)."Cybersecurity and Physical Security Convergence." https://www.cisa.gov/sites/default/files/publications/Cybersecurity%20and%20Physical%20Security%20Convergence_508_01.05.2021_0.pdf (accessed March 10, 2022).

Cybersecurity and Infrastructure Security Agency (CISA)." Security Tip (ST04-001) What is Cybersecurity?" November 14, 2019. https://www.cisa.gov/uscert/ncas/tips/ST04-001 (accessed February 5, 2022).

Cybersecurity and Infrastructure Security Agency. (CISA) "CISA Cybersecurity Advisory Committee." February 1, 2022 https://www.cisa.gov/cisa-cybersecurity-advisory-committee (accessed February 18, 2022).

Cybersecurity and Infrastructure Security Agency (CISA). "Transportation Systems Sector." https://www.cisa.gov/transportation-systems-sector (accessed March 7,2022).

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 February 18, 2022).

Cybersecurity and Infrastructure Security Agency (CISA). "Information and Communications Technology (ICT) Supply Chain Risk Management (SCRM) Task Force." https://www.cisa.gov/ict-scrm-task-force (accessed March 8, 2022).

Cybersecurity and Infrastructure Security Agency (CISA). "Information and Communications Technology (ICT) Supply Chain Risk Management (SCRM)" https://www.cisa.gov/supply-chain (accessed January 31, 2022).

Cybersecurity and Infrastructure Security Agency (CISA). "National Risk Management." https://www.cisa.gov/national-risk-management (accessed January 31, 2022).

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 7, 2022).

Department of Defense (DoD) Zero Trust Reference Architecture. February 2021. https://dodcio.defense.gov/Portals/0/Documents/Library/(U)ZT_RA_v1.1(U)_Mar21.pdf (accessed February 15, 2022).

Department of Defense. "Strategic Directions for Cybersecurity Maturity Model (CMMC) Program." November 4, 2021. https://www.defense.gov/News/Releases/Release/Article/2833006/strategic-direction-for-cybersecurity-maturity-model-certification-cmmc-program/ (accessed March 11, 2022).

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 18, 2022).

Department of Homeland Security. Information Circular: "Surface Transportation IC-2021-01: Enhancing Surface Transportation Cybersecurity." December 31, 2021. https://www.tsa.gov/sites/default/files/20211201_surface-ic-2021-01.pdf (accessed February 9, 2022).

Department of Homeland Security. Security Directive 1582-21-01 "Enhancing Public Transportation and Passenger Railroad Cybersecurity." December 2, 2021. https://www.tsa.gov/sites/default/files/sd-1582-21-01_signed.pdf (accessed February 9, 2022).

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 March 11, 2022).

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

"Enhancing Cybersecurity in Public Transportation," National Center for Transit Research (NCTR) Report. No CUTR_NCTR_RR-1018-04, Center for Urban Transportation Research, University of South Florida. 2018. DOI: https//doi.org/10.5038/CUTR-NCTR-RR-2018-04 (accessed February 16, 2021).

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 March 16, 2022).

Federal Transit Administration (FTA). "Triennial Reviews." January 27, 2022 https://www.transit.dot.gov/funding/grantee-resources/triennial-reviews/triennial-reviews (accessed March 16,2022).

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).

Frick, Karen Trapenberg, Giselle Mendonca Abreu, Nathan Malkin, Alexandra Pan, Alison Post, *The Cybersecurity Risks of Smart City Technologies.* February 2021 https://cltc.berkeley.edu/wp-content/uploads/2021/03/Smart_City_Cybersecurity.pdf (accessed February 8, 2022).

GITHUB "01-Principles of Security Engineering.md." https://github.com/OWASP/DevGuide/blob/master/02-Design/01-Principles%20of%20Security%20Engineering.md (accessed February 8, 2022).

IBM *Cost of a Data Breach Report 2021.* 4,8 July 2021. https://www.ibm.com/downloads/cas/OJDVQGRY (accessed February 1, 2022).

International Organization for Standardization (ISO), "ISO/IEC 27002 Information Security Management." https://www.iso.org/isoiec-27001-information-security.html (accessed February 8, 2022).

KnowBe4. Economic Impact of Cyber Attacks on Municipalities. https://www.knowbe4.com/hubfs/Cyber-Attacks-on-Municipalities-White-Paper.pdf (accessed February 16, 2022).

National Academies of Sciences, Engineering, and Medicine 2022. *Cybersecurity in Transit Systems,* Washington DC: The National Academies Press. https://doi.org/10.17226/26475 (accessed February 10, 2022).

National Academies of Sciences, Engineering, and Medicine 2020. *Update of Security 101: A Physical and Cybersecurity Primer for Transportation Agencies.* Washington, DC. The National Academies Press. https://doi.org/10.17226/25554 (accessed March 8, 2022).

National Academies of Sciences, Engineering, and Medicine 2016. *Protection of Transportation Infrastructure from Cyber Attacks: A Primer.* Washington, DC. The National Academies Press. https://doi.org/10.17226/23516 (accessed February 8, 2022).

National Highway Traffic Safety Administration (NHTSA). Cybersecurity Best Practices for Modern Vehicles. October, 2016. (Report No. DOT HS 812 333). https://www.nhtsa.gov/staticfiles/nvs/pdf/812333_CybersecurityForModernVehicles.pdf (accessed January 31, 2022).

https://www.nhtsa.gov/sites/nhtsa.gov/files/documents/vehicle_cybersecurity_best_practices_01072021.pdf

National Institute of Standards and Technology (NIST) "SCRC Glossary Cyber Resiliency." https://csrc.nist.gov/glossary/term/cyber_resiliency (accessed February 4, 2022)

National Institute of Standards and Technology (NIST) Computer Security Resource Center. "NIST Risk Management Framework." March 16, 2022, https://csrc.nist.gov/projects/risk-management; (accessed March 16, 2022).

National Institute of Standards and Technology (NIST) "SP 800-53 Rev. 5: Security and Privacy Controls for Information Systems and Organizations." December 10, 2020. https://csrc.nist.gov/publications/detail/sp/800-53/rev-5/final (accessed March 10, 2022).

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. April 16, 2018. https://nvlpubs.nist.gov/nistpubs/CSWP/NIST.CSWP.04162018.pdf (accessed February18, 2022).

National Institute of Standards and Technology (NIST). "The Five Functions." May 12, 2021. https://www.nist.gov/cyberframework/online-learning/five-functions (accessed February 8, 2022).

National Institute of Standards and Technology (NIST) "Cybersecurity." https://www.nist.gov/cybersecurity (accessed March 1, 2022).

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 CybersecurityInformation Sharing. *80 FR 9347*. February 20, 2015.

Office of Management and Budget. "Memorandum For The Heads of Executive Departments and Agencies: Moving the U.S. Government Toward Zero Trust Cybersecurity Principles. January 26, 2022. https://www.whitehouse.gov/wp-content/uploads/2022/01/M-22-09.pdf (accessed March 10, 2022).

Office of the Undersecretary of Defense – Acquisition & Sustainment. "Securing the Defense Industrial Base CMMC 2.0." https://www.acq.osd.mil/cmmc/ (accessed February 8, 2022).

Transportation Security Administration (TSA) Enhancing Public Transportation and Passenger Railroad Cybersecurity Security Directive 1582-21-01:December 31, 2021, https://www.tsa.gov/sites/default/files/sd-1582-21-01_signed.pdf (accessed March 8, 2022).

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 1, 2022).

Transportation Security Administration (TSA). "Cybersecurity Roadmap 2018." November 2018. https://www.tsa.gov/sites/default/files/documents/tsa_cybersecurity_roadmap.pdf (accessed March 15, 2022).

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 1, 2022).

Trump, Donald J. Executive Order-13800. Strengthening the Cybersecurity of FederalNetworks 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 Congress, Public Law 117-58. November 15, 2021. https://www.congress.gov/117/plaws/publ58/PLAW-117publ58.pdf (accessed February 24, 2022.

United States House of Representatives, HR 3359 Cybersecurity and Infrastructure Security Agency Act of 2018. November 16, 2018, https://www.congress.gov/bill/115th-congress/house-bill/3359 (accessed March 3, 2022).

United States Congress, Public Law 117-103. March 15, 2022. https://www.congress.gov/bill/117th-congress/house-bill/2471 (accessed May 14, 2022)

United States Senate, Committee on Homeland Security and Government Affairs, *Federal Cybersecurity Still at Risk*, August 2021, https://www.hsgac.senate.gov/imo/media/doc/Federal%20Cybersecurity%20-%20America's%20Data%20Still%20at%20Risk%20(FINAL).pdf (accessed March 3, 2022).

The White House. "Statement by the President on S. 1605, the National Defense Authorization Act of Fiscal Year 2022." December 27, 2021. https://www.whitehouse.gov/briefing-room/statements-releases/2021/12/27/statement-by-the-president-on-s-1605-the-national-defense-authorization-act-for-fiscal-year-2022/ (accessed March 2, 2022).

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.

Kathryn Seckman, MA

Kathryn Seckman is the Executive Director of Strategy and Analysis at Grayline Group where she partners with organizations to lead purposeful disruption, craft strategic communications, and enable informed decision making. She began her career analyzing transnational threats, leading due diligence assessments, and providing geopolitical risk advisory services to Fortune 100 companies across multiple industries. Ms. Seckman most recently was with General Motors Company, where in 2017 she joined the Global Public Policy team at headquarters in Detroit, Michigan. She was responsible for leading analysis on global trade policy and tariff impacts, as she worked across business units to align business and policy objectives. She participated in national labor negotiations, wrote strategy alignment briefs for Policy, Legal, Manufacturing, and Labor senior executives, and led critical support and communications for CEO engagement in key business associations and boards. She subsequently developed a Workforce Strategy portfolio for GM's Global Human Resources team, leading the cross-functional strategy design and implementation of inclusive "future of work" principles. Ms. Seckman is a Fulbright Scholar, holds an MA in Security Studies from Georgetown University, and a BA in International Relations from Drake University.

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." 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. Mr. Thomas received his BA from The George Washington University and his MBA from the University of Texas at Austin.

Homayun Yaqub, MA

Homayun Yaqub brings more than 25 years of security and risk management experience in the public and private sectors. Mr. Yaqub was a Global Security Strategist at Forcepoint and has led multiple risk and security initiatives at JPMorgan Chase & Company. As an independent consultant, Mr. Yaqub advised Global 1000 companies on strategies to better manage risk and enhance their security posture. He was also a founding member of The MASY Group, a global security and risk consulting firm, and has held multiple leadership and executive roles in the Department of Defense and U.S. Intelligence Community.

MTI FOUNDER

Hon. Norman Y. Mineta

MTI BOARD OF TRUSTEES

Directors