TRANSIT ADVISORY COMMITTEE FOR SAFETY (TRACS)

2022–2024 Charter

CYBER AND DATA SECURITY REPORT

CREATING A TRANSIT CYBER AND DATA SECURITY BASELINE

REPORT 22-03

2/1/2024

Table of Contents

Executive Summary

Public transportation is deeply woven into American society. As public transportation systems and resources are digitized and connected, more opportunities arise for malicious actors to disrupt operations on a massive and potentially catastrophic scale. Transit agencies of all sizes should implement cybersecurity practices to prevent these potential disruptions.

The TRACS cyber and data security subcommittee met several times throughout 2023 to discuss ways FTA could improve the cybersecurity hygiene for transit agencies. The subcommittee found that cybersecurity is regulated by the Department of Homeland Security (DHS) and its components. DHS charges the Transportation Security Administration (TSA) with securing the nation's transportation systems, which includes mass transit agencies. TSA has set transit cybersecurity requirements for large rail agencies but has not established requirements for small or medium-sized agencies or transit bus only agencies. However, FTA can create recommendations, guidelines, tools, or resources for use by transit agencies to help improve their cybersecurity posture.

The TRACS cyber and data security subcommittee developed seven recommendations, summarized in the table below. These recommendations were developed to improve the cybersecurity hygiene for all agencies but are expected to have the greatest impact for small and medium size agencies that do not have the resources of large agencies. Each recommendation is followed by implementation suggestions, which FTA can consider as actionable strategies to implement the recommendation.

TRACS Recommendation for FTA	Implementation Suggestions
Recommendation 1: Define FTA's cybersecurity role	1. FTA should clarify and formalize its cybersecurity role. 2. Create and maintain an open line of communication with TSA. 3. Consider the scalability of cybersecurity recommendations and guidelines.
Recommendation 2: Summarize existing rules, regulations, and guidance and outline agency reporting requirements	1. Create a summary of existing rules, regulations, and guidelines for transit agencies. 2. Create a document detailing cyberattack reporting requirements for agencies.
Recommendation 3: Encourage cybersecurity integration into transit agencies	1. Perform a gaps analysis. 2. Create and encourage agencies to complete a cybersecurity hygiene baseline tool. 3. Consider cybersecurity in the SRM process of an agency's PTASP. 4. Encourage agencies to create a post-cyberattack recovery plan. 5. Provide cybersecurity technical assistance.
Recommendation 4: Create a cybersecurity awareness course	1. Create a transit cybersecurity course. 2. Recommend transit agencies take the cybersecurity course.
Recommendation 5: Create products, services, and vendors procurement guidance	1. Create product, service, and vendor procurement guidance. 2. Create standard RFP language.

TRACS Recommendation for FTA	Implementation Suggestions
Recommendation 6: Create a library of cybersecurity resources	1. Create a transit cybersecurity resource library. 2. Identify a group responsible for managing the library.
Recommendation 7: Develop and fund cybersecurity research topics	1. Develop research topics. 2. Perform or fund cybersecurity research. 3. Publish and promote the research.

TRACS Members

Name	Agency/Organization
Edward Abel	Southeastern Pennsylvania Transportation Authority
Brian Alberts**	American Public Transportation Association (APTA)
Johanna Cockburn*	City of Greensboro (NC)
Enjoli DeGrasse	International Brotherhood of Teamsters
Beverly Edwards	First Transit
Rebecca Frankhouser	King County Metro (WA)
David Harris*	New Mexico Department of Transportation (DOT)
Molly Hughes*	Washington State DOT
Donna Johnson	Dallas Area Rapid Transit
Laura Karr	Amalgamated Transit Union
James Keane*	New Jersey Transit (NJT)
Thomas Lamb	Metropolitan Transportation Authority, New York City Transit
Brian Lapp	Port Authority of New York and New Jersey
Raymond Lopez	Los Angeles County Metropolitan Transportation Authority
Rachel Maleh	Operation Lifesaver, Inc.
Santiago Osorio	Metropolitan Transit Authority of Harris County (TX)
Karen Philbrick*	Mineta Transportation Institute, San Jose State University
Ashley Porter*	Florida DOT
Patrick Preusser	Department of Transportation Services City and County of Honolulu
Reggie Reese	Pierce Transit (WA)
Adam Sharkey	River Cities Public Transit (SD)
Justin Sobeck*	Missouri DOT
Lisa Staes*	Center for Urban Transportation Research, University of South Florida
Gardner Tabon	Capital Metropolitan Transportation Authority (TX)
Curtis Tate	Transport Workers Union of America

* Cyber and Data Subcommittee member
** Cyber and Data Subcommittee chair

Introduction

Cybersecurity is the practice of protecting computer systems, networks, and other digital devices from unauthorized access or attack.[1] There is growing concern for public transit agencies about the risk of cyberattacks as control and management systems become increasingly connected and dependent on information technology (IT) and operational technology (OT) systems. With the increased digitization, more opportunities arise for malicious actors and system malfunctions to disrupt operations on a massive and potentially catastrophic scale.[2] Types of sophisticated direct and indirect cyberattacks from malicious actors can include viruses, malware, phishing scams, and hacking attempts.[3] These threats can cause serious damage to both individuals and organizations by stealing personal data or compromising important systems.[4] To effectively combat these threats, cybersecurity puts a variety of tools and techniques in place, including firewalls, antivirus software, and workforce education.[5]

Background on Cybersecurity and Transit

Transit Cybersecurity

Transit agencies recognize that cybersecurity is a growing concern for which appropriate actions are urgent and required to reduce operational and financial risk.[6] Transit agencies have both IT and OT systems that are vulnerable to cyberattacks. Transit agency operational technology (OT) systems are the industrial control systems (ICS) that support operational services such as train control systems, traffic control systems, closed-loop passenger access systems and other operational services while IT devices manage the flow of agency data. With the growing dependence on technology by governments, businesses, individuals, and networks linking to end users, cyberspace is increasingly becoming an attractive target to malicious actors.[7]

Modern transit systems are heavily dependent on various IT systems and therefore are naturally at risk of a broad spectrum of cyberthreats. Typically, a transportation agency's IT infrastructure consists of three general layers:

---

[1] Cyber Security Degrees & Career Guide. Do You Need Coding for Cyber Security. June 3, 2023. https://cybersecuritycareer.org/do-you-need-coding-for-cyber-security/

[2] Mineta. Is the Transit Industry Prepared for the Cyber Revolution? Policy Recommendations to Enhance Surface Transit Cyber Preparedness. September 2020. https://transweb.sjsu.edu/research/1939-Transit-Industry-Cyber-Preparedness

[3] APTA. Cybersecurity Considerations for Public Transit, APTA SS-ECS-RP-001-14. July 29, 2022. https://www.apta.com/wp-content/uploads/APTA-SS-ECS-RP-001-14_R1.pdf

[4] Cyber Security Degrees & Career Guide. Do You Need Coding for Cyber Security. June 3, 2023. https://cybersecuritycareer.org/do-you-need-coding-for-cyber-security/

[5] Cyber Security Degrees & Career Guide. Do You Need Coding for Cyber Security. June 3, 2023. https://cybersecuritycareer.org/do-you-need-coding-for-cyber-security/

[6] APTA. Cybersecurity Considerations for Public Transit, APTA SS-ECS-RP-001-14. July 29, 2022. https://www.apta.com/wp-content/uploads/APTA-SS-ECS-RP-001-14_R1.pdf

[7] APTA. Cybersecurity Considerations for Public Transit, APTA SS-ECS-RP-001-14. July 29, 2022. https://www.apta.com/wp-content/uploads/APTA-SS-ECS-RP-001-14_R1.pdf

1. **Operational systems**: These systems integrate supervisory control and data acquisition (SCADA), original equipment manufacturer (OEM), and other critical component technologies responsible for the supervision, movement, and monitoring of transportation equipment and services (e.g., train, track and signal control). Often, such systems are interrelated into multimodal systems such as buses, ferries, paratransit, and metro modes.
2. **Enterprise information systems**: A transit agency's enterprise information system consists of the integrated layers of the operating system, applications systems, and business system. Holistically, enterprise information systems encompass the entire range of internal and external information exchange and management.
3. **Subscribed systems**: These consist of "managed" systems outside the transportation agency. Such systems may include internet service providers, hosted networks, the agency website, data storage, and cloud services.

Over 70 percent of agencies surveyed say they have not yet had many (or any) cybersecurity incidents; however, research suggests that this statistic should be inverted, and that the large majority of organizations have experienced cybersecurity incidents.[8] Cyberattacks can destroy a transit agency's physical systems, render them inoperable, hand over control of those systems to an outside entity, or jeopardize employee or customer data privacy. With the unprecedented pace and complexity of cyberattacks, a transit agency must be proactive in the strategic adoption of a holistic cybersecurity approach to protect critical information and fulfill its obligation to its customers.[9]

Forms of Cyberattacks

Cyberattacks can take many forms. Many cyberattacks are known to exploit specific hardware linked to the IT ecosystem like manipulating infrared devices, jamming Wi-Fi signals, or even physically tapping or damaging critical communication cabling or nodes. Additionally, while many cyberattacks may be external, transit agencies, just like any other organization, are susceptible to internal attacks, such as from a disgruntled employee. An attack from an internal source has a higher probability of success and a more significant potential for damage, given the level of access and knowledge an insider may possess. Common cyberattacks forms include the following:[10, 11]

- **Social engineering:** The art of manipulating individuals' trust, behavior, or identity. The individuals being manipulated can be uniformed or untrained employee who do not understand cyber risks.

[8] Mineta. Is the Transit Industry Prepared for the Cyber Revolution? Policy Recommendations to Enhance Surface Transit Cyber Preparedness. September 2020. https://transweb.sjsu.edu/research/1939-Transit-Industry-Cyber-Preparedness
[9] APTA. Cybersecurity Considerations for Public Transit, APTA SS-ECS-RP-001-14. July 29, 2022. https://www.apta.com/wp-content/uploads/APTA-SS-ECS-RP-001-14_R1.pdf
[10] APTA. Cybersecurity Considerations for Public Transit, APTA SS-ECS-RP-001-14. July 29, 2022. https://www.apta.com/wp-content/uploads/APTA-SS-ECS-RP-001-14_R1.pdf
[11] CISA. 2022 Top Routinely Exploited Vulnerabilities. August 3, 2023. https://www.cisa.gov/news-events/cybersecurity-advisories/aa23-215a

- **Exploitation of hardware and software coding:** While cyberattacks in the form of software manipulation require a degree of expertise and technical knowledge, physical manipulation (intentional and unintentional) of the system is also of genuine concern. Once the targeted system is compromised, perpetrators might implement "backdoor" gates or install stealth code, allowing data to be monitored or removed without detection.
- **Ransomware:** Ransomware is an ever-evolving form of malware designed to encrypt files on a device, rendering any files and the systems that rely on them unusable. Malicious actors then demand a ransom in exchange for decryption. Ransomware actors often target and threaten to sell or leak exfiltrated data or authentication information if the ransom is not paid.

Existing Recommended Actions

To help mitigate the growing cyberthreat against transit agencies, organizations like APTA have created a list of recommended actions that encourage transit agencies to incorporate cybersecurity into their organization. APTA's recommendations include:[12, 13]

- Involving executive-level leadership in the cybersecurity program.
- Keeping operating systems, software, and antivirus products up to date.
- Disabling unnecessary remote desktop protocol (RDP) connections.
- Training staff to protect themselves against phishing attacks.
- Maintaining regular backups of system data.
- Reviewing and enforcing policies on backups, patching, access controls, encryption, and passwords.
- Educating employees about the risks of disinformation, phishing, spear phishing, best practices for password management, and internet safety.
- Monitoring and protecting agency data.
- Securing cross-domain connectivity and dispersed infrastructure.
- Planning for the worst-case scenario and considering potential extortion scenarios.
- Putting in place business continuity and disaster recovery plans.
- Ensuring that incident response capabilities are readily available.
- Having a clear media strategy.
- Running regular exercises with all relevant stakeholders.
- Obtaining a vulnerability assessment of the network environments.

However, despite APTA's publication of these recommended agency actions, many agencies do not have a robust cybersecurity program. To help these agencies improve their cybersecurity posture, TRACS developed a list of recommendations for FTA.

[12] APTA. Cybersecurity Considerations for Public Transit, APTA SS-ECS-RP-001-14. July 29, 2022. https://www.apta.com/wp-content/uploads/APTA-SS-ECS-RP-001-14_R1.pdf
[13] APTA. Security and Emergency Management Standards. https://www.apta.com/research-technical-resources/standards/security/

Federal Cybersecurity Activities

Cybersecurity for transit is primarily regulated by the Transportation Security Administration (TSA), but applicability is currently limited. TSA has established transit cybersecurity requirements through Security Directives for large rail agencies and voluntary guidance for all others, including small- or medium-sized transit agencies. Transit agencies may also be affected by the Cyber Incident Reporting for Critical Infrastructure Act of 2022. This Act requires the Cybersecurity and Infrastructure Security Agency (CISA) to develop and implement regulations for covered entities to report cyber incidents and ransomware payments to CISA. To support cybersecurity enhancement, TSA has created tools and guidelines that agencies of all sizes can use, like its Baseline Assessments for Security Enhancement (BASE) Assessment. A BASE Assessment is a free, voluntary, risk-based program that evaluates the security posture of transportation systems. BASE aids mass transit operators in elevating their security posture by implementing and sustaining baseline security measures applicable to their operating environments and specific system characteristics.[14] CISA created the Cyber Resilience Review (CRR), which is a voluntary interview-based assessment agencies can use to evaluate an organization's operational resilience and cybersecurity practices.[15]

While TSA *regulates* cybersecurity, other agencies—like FTA and APTA— developed cybersecurity tools, guidelines, and recommendations for agencies to use. APTA uses National Institute of Standards and Technology (NIST) standards to better define the critical actions transit agencies should take to secure transportation networks. FTA created the Cybersecurity Assessment Tool for Transit (CATT), which assists public transit agencies in formalizing and developing their cybersecurity programs.[16]

TRACS Recommendations for FTA

The Subcommittee found that there are many freely available guidelines, recommendations, and tools for transit agencies to use to improve their cybersecurity hygiene. However, the Subcommittee developed several recommendations for FTA that can help improve the cybersecurity posture specifically for transit agencies. While these recommendations were developed with all agencies in mind, the Subcommittee expects them to have the greatest impact for small and medium-sized agencies that do not have the resources of large agencies. The following sections provide in-depth information on each recommendation developed by the Subcommittee.

[14] TSA. TSA Releases Baseline Assessments for Security Enhancement (BASE) Benchmarking Report for Mass Transit, January 21, 2021. https://exis.tsa.dhs.gov/NewsDetail.aspx?oVjwVsovK/CAHtdU+CnYVleMcLR0uuHjrkN+ZDo8pONm/feYl7ca3anj46v5Lrc7V+Kbk2QXu+RDiucNwuK63g==

[15] APTA. Cybersecurity Considerations for Public Transit, APTA SS-ECS-RP-001-14, July 29, 2022. https://www.apta.com/wp-content/uploads/APTA-SS-ECS-RP-001-14_R1.pdf

[16] FTA. Cybersecurity Assessment Tool for Transit (CATT), June 21, 2023. https://www.transit.dot.gov/research-innovation/cybersecurity-assessment-tool-transit-catt

Recommendation 1: Define FTA's Cybersecurity Role

Background of Subcommittee Findings

Cybersecurity regulations fall under the jurisdiction of TSA, which has already set requirements for large passenger and freight rail agencies. The Subcommittee believes that FTA can help transit agencies that do not have TSA cybersecurity requirements (like smaller rail transit agencies or bus-only agencies) by encouraging them to incorporate cybersecurity into their agencies. FTA can accomplish this by performing actions like the recommendations detailed in this paper, which include creating recommendations, guidance, tools, and trainings. Any recommendations or guidance created by FTA should slowly be rolled out to with ample guidance and tools in the beginning so that smaller agencies are not overburdened by regulations in this area. However, if FTA does create recommendations and guidance, agency regulatory authority needs to be carefully considered to avoid an overreach of authority. Additionally, FTA can use its close connections and knowledge of local transit agencies to ensure that these smaller agencies are aware of future TSA cybersecurity requirements that apply to them, and to advise TSA on any cybersecurity recommendations or recommendations it sets for smaller agencies.

Any recommendations or guidelines that FTA creates should align with existing TSA requirements. However, before creating recommendations and guidance, FTA should:

- Carefully consider how it wants to help transit agencies in the cybersecurity space.
- Create and maintain an open line of communication with TSA where recommendations and guidance can be discussed.
- Carefully consider the scalability of any recommendations and guidance it sets.

Implementation Suggestions

The Subcommittee believes TSA can play a vital role for medium- and small-sized rail transit agencies and all bus agencies because these agencies are not being regulated by TSA as of December 2023. Subcommittee recommended actions for FTA include the following:

1. FTA should clarify and formalize its cybersecurity role.

The Subcommittee recommends that FTA clarifies and formalizes its oversight of cyber safety and how it is different from cybersecurity, which is regulated by TSA. This recommendation is made so state safety oversight agencies and their funding sub-recipients can have the local authority to follow any cybersecurity recommendations and guidelines FTA sets.

The Subcommittee also recommends that FTA clearly defines its role compared to the role of TSA. Both TSA and FTA can have a role in providing cybersecurity recommendations and guidance for transit agencies. TSA has the authority to set cybersecurity rules and regulations, while FTA can create recommendations and guidelines for transit agencies. A clearly defined role will help small- and medium-sized agencies clearly understand which regulations they need to follow and which agency they come from.

2. Create and maintain an open line of communication with TSA.

The Subcommittee recommends that FTA maintains an open line of communication with TSA, like FTA has been doing during its reoccurring meetings. FTA should use this open line of communication to make TSA aware of any recommendations or guidelines it establishes for transit agencies of any size.

3. Consider the scalability of cybersecurity recommendations and guidelines.

The Subcommittee recommends that any cybersecurity recommendations and guidelines created by FTA should be carefully thought out to determine if they are scalable and achievable for agencies of all different sizes. Many small- to medium-sized transit agencies do not have a robust cybersecurity department or cybersecurity resources. FTA should also discuss the issue of scalability with TSA so it understands that any rules and regulations it sets need to be achievable for these smaller agencies.

Recommendation 2: Summarize Existing Rules, Regulations, and Guidance and Outline Agency Reporting Requirements

Background of Subcommittee Findings

TSA sets cybersecurity rules and regulations for larger passenger and freight agencies, but small and medium-sized agencies and bus-only agencies are still required to report cyberattacks. However, these small- and medium-sized agencies often lack the cybersecurity resources that large agencies have and are not aware that they have to report cyberattacks or to whom they have to report. Additionally, because the rules that are set vary by agency size, type of attack, and agency impact severity, many transit agencies do not know if cybersecurity requirements apply to their agency or even what their cybersecurity requirements are.

To help alleviate agency confusion and help agencies understand the existing cybersecurity requirements, FTA can concisely summarize existing rules, regulations, and guidance for transit agencies of all types and sizes. FTA can also create a document summarizing cyberattack reporting requirements for these agencies. Note that these summaries will help FTA understand what requirements exist and what gaps it can fill.

Implementation Suggestions

1. Create a summary of existing rules, regulations, and guidelines for transit agencies.

The Subcommittee recommends that FTA creates a document or table summarizing existing rules, regulations, and guidance for transit agencies of all types and sizes. The summary should help agencies clearly understand what cybersecurity rules, regulations, and guidelines exist today and which ones explicitly apply to them. This summary can include both items that are required and items that offer cybersecurity guidance. Note that this summary can also help inform FTA what regulations or guidelines it could create that would be impactful.

2. Create a document detailing cyberattack reporting requirements for agencies.

The Subcommittee recommends that FTA create a document such as a matrix or table detailing reporting requirements for agencies that experience a cyberattack. The reporting requirements can cover a variety of topics, like what to report if the agency faced a cyberattack, who it should immediately report to (e.g. the Federal Bureau of Investigation, TSA, or local law enforcement), and general annual review reporting requirements. The documentation can also include clear data collection and reporting requirements for agencies. The document should also be printable so agencies that experience a cyberattack can access a physical copy of the document.

Recommendation 3: Encourage Cybersecurity Integration into Transit Agencies

Background and Subcommittee Findings

Many transit agencies, especially small- to medium-sized agencies, do not have robust cybersecurity standards or requirements. The Subcommittee found that transit agencies have individual reasons for not implementing these cybersecurity standards or requirements which are often a combination of funding, thinking cybersecurity is too complicated, not understanding the guidelines and tools available to them, having a risk tolerance for cyberattacks, thinking cyberattacks are rare and unlikely to happen to their agency, or even thinking cybersecurity is not a serious risk to their agency. To make these small- and medium-sized agencies aware of cybersecurity and encourage agencies to incorporate cybersecurity, FTA can do the following:

- Perform a cybersecurity gaps analysis.
- Create a cybersecurity hygiene baseline tool targeting small- and medium-sized transit agencies.
- Incorporate a cybersecurity component into the Public Transportation Agency Safety Plans (PTASP).
- Encourage agencies to create a post-cyberattack recovery plan.
- Provide technical assistance.

Implementation Suggestions

1. Perform a gaps analysis.

The Subcommittee recommends that FTA uses the research work performed for Recommendation 1 to conduct a gaps analysis. The gaps analysis can be used by FTA to understand the current state of transit cybersecurity and what items are missing from the recommended state. FTA can also use this analysis to understand what tools, recommendations, and guidance might be needed by transit agencies that do not have TSA cybersecurity requirements.

2. Create and encourage agencies to complete a cybersecurity hygiene baseline tool.

The Subcommittee recommends that FTA creates a cybersecurity hygiene baseline tool for transit agencies that provides the agency a high-level overview of their cybersecurity capabilities, and easy-to-accomplish actions the agency can take to improve their cybersecurity posture. The hygiene tool should

be developed in a way that small- and medium-sized agencies that do not have robust cybersecurity resources can complete it without much assistance. The tool can pull information from existing cybersecurity baseline tools like CRR, CATT, or BASE.

3. Consider cybersecurity in the SRM process of an agency's PTASP.

The Subcommittee would like transit agencies to consider incorporating a cybersecurity component into the SRM process of their PTASP. This inclusion should help agencies become more aware of cybersecurity threats, their potential harm, and ways to respond to and prevent cyberattacks. To help with this inclusion of cybersecurity, small- and medium-sized agencies can use cybersecurity resources from other agencies and the FTA, including the resources recommended by the Subcommittee. The Subcommittee recommends that transit agencies consider cybersecurity in the SRM process. The Subcommittee also recommends that FTA reach out to the transit industry to gather feedback on the burden that incorporating a cybersecurity component into the SRM process of their PTASP would place on agencies.

The Subcommittee noted that this requirement comes with challenges, such as cybersecurity not falling directly under the purview of the transit agency, and the PTASP containing potential private information. To overcome these challenges, FTA can clarify and formalize its cybersecurity role, as suggested in Recommendation 1, and provide agencies with cybersecurity recommendations and best practices or create links that will take the agencies to existing resources like CRR or CATT. Additionally, the agency's PTASP can reference a security plan or other cybersecurity document to avoid directly publishing sensitive information.

4. Encourage agencies to create a post-cyberattack recovery plan.

The Subcommittee recommends that FTA encourages transit agencies to create a cyberattack recovery plan. These plans should list (or be a checklist of) steps an agency should take to bounce back after a cyberattack. The plan should include steps that are technical and programmatic, including media communication tools. The Subcommittee believes that these recovery plans should be printed by the agency so that in the event of a cyberattack, the plan is not lost.

5. Provide cybersecurity technical assistance.

To help the small- and medium-sized transit agencies integrate cybersecurity into their agencies, FTA should provide a cybersecurity technical assistance center. The technical assistance center should be set up to meet the needs of the transit agencies. The Subcommittee feels that the technical assistance center should be set up as an advising center for agencies—specifically, as a hotline to call if there is a cyberattack. The call center can perform tasks like reviewing cybersecurity documents, answering technical and programmatic questions, and even assisting an agency with testing its cybersecurity systems. This technical assistance could be set up like the PTASP technical assistance center.

Recommendation 4: Create a Cybersecurity Awareness Course

Background and Subcommittee Findings

Many transit agencies do not offer cybersecurity training to their employees. There are some cybersecurity courses available for free, but they are not required and are not transit focused. The Subcommittee found that about 90 percent of cybersecurity attacks are caused by exploiting employees of an organization.[17] For example, an attacker could contact an organization's human resources department head and request sensitive employee data like social security numbers. Employees should be trained by the agency to identify attacks like this and actions they should take if they encounter a threat like this. FTA can create a cybersecurity course for transit agencies to give to their employees that addresses these needs.

Implementation Suggestions

1. Create a transit cybersecurity course.

The Subcommittee recommends that FTA creates a transit-focused cybersecurity course that covers cybersecurity basics and transit vulnerabilities. The information in this course should align with and can be modeled on the FTA and Transportation Safety Institute (TSI) basic 2-hour Safety Measurement System (SMS) online training. The course should target agency staff and make them aware of basic cybersecurity procedures, including the following:

- The relationship between the cyber vulnerability and the potential consequences of a successful cybersecurity attack, including the types of data that can be compromised and who can be impacted, such as the traveling public and not just the agency employees.
- How to identify a cybersecurity threat (e.g., a phishing email or a spoof call).
- What to do if they believe they are the target of a cybersecurity attack.
- Standard operating procedures for reporting a cybersecurity attack.
- Creating a non-punitive culture of reporting cybersecurity attacks.

This course should be marketed to all transit agencies, especially small- and medium-sized agencies that do not have a cybersecurity department, and should encourage the agencies to administer the training annually. Additionally, FTA could create separate cybersecurity courses for different types of agencies, like rail or bus agencies. The transit cybersecurity course could be created and managed by the National Highway Institute (NHI) or the TSI.

2. Recommend transit agencies take the cybersecurity course.

The Subcommittee recommends that FTA recommends the transit cybersecurity course to all transit agency employees, including contractors. This training can be a supplemental course for agencies to adopt if they do not already have a cybersecurity basics training. However, if the transit agency already

[17] CISA. Stop Ransome Ware General Information. https://www.cisa.gov/stopransomware/general-information

has a cybersecurity course that its employees are required to take, the agency should be able to use its own course if it covers, at a minimum, all the information in the FTA course.

Recommendation 5: Provide Cybersecurity Guidance for Procuring IT and OT Products and Services

Background of Subcommittee Findings

Many agencies require assistance when procuring cybersecurity devices and services. Agencies of different sizes have staff with different cybersecurity knowledge levels and resources, with some agencies having dedicated cybersecurity departments and other agencies rolling cybersecurity responsibilities into their IT or engineering departments.

The Subcommittee found that the small- and medium-sized agencies could use help procuring cybersecurity devices and services, or operational devices and services that interact with their IT systems. Often, these agencies do not have a dedicated cybersecurity department, so being able to find reputable vendors and products can be a challenge. Once the devices are purchased, these agencies may not know how to test the devices or services to verify that they are performing the required tasks.

Implementation Suggestions

1. Create product and service procurement guidance.

The Subcommittee recommends that FTA creates freely available product and service procurement guidance for cybersecurity devices. This guidance should be scalable for agencies of different sizes and should be simple for agencies to follow, like a list of questions the agencies should ask to ensure that devices, services, and contractors are cyber secure. The guidance can include the following:

- How to find reputable and trustworthy vendors, services, and products.
- How to test services and products to ensure that they meet the minimum standards, and what these minimum standards are or how to find them.
- How to ensure device, service, or agency interoperability.

The guidance should also align with any cybersecurity guidance TSA has already created and should be scalable for agencies of different sizes. The guidance can also separate out IT and OT needs and different types of procurement, like rail cars, cameras, and cybersecurity oversight services.

2. Create standard request for proposal (RFP) language.

The Subcommittee recommends that FTA creates standard language that agencies can add to their RFPs that encourages cybersecurity screening of parts, products, and vendors. The Subcommittee noted that a transit agency recently purchased devices from another country which were pre-hacked and had to be discarded. Having standard RFP language could help the agency mitigate the financial and operations impacts of threats like this.

Recommendation 6: Create a Library of Cybersecurity Resources

Background of Subcommittee Findings

The Subcommittee found that many agencies do not know where to look for cybersecurity resources. The agencies often rely on search engine results, which often point to private company websites or websites that do not apply to transit cybersecurity.

To help agencies find cybersecurity resources, FTA could create a one-stop-shop library for cybersecurity resources. These resources could include existing rules, regulations, and guidance, but can also include general cybersecurity references and tools, such as the TSA and FTA cybersecurity hygiene assessment tools. These resources could tie to the summaries of existing rules, regulations, and guidance and outline agency reporting requirements, as noted in Recommendation 2.

Implementation Suggestions

1. Create a transit cybersecurity resource library.

The Subcommittee recommends that FTA creates a transit cybersecurity library that serves as the primary location for finding cybersecurity resources and tools. To add value to the library, the resources stored here should tie to the agency requirements. FTA should also clearly identify what this clearinghouse would include, how frequently it would be updated, and how the resources would be amplified.

2. Identify a group responsible for managing the library.

The Subcommittee recommends that FTA identifies a group, university, or agency that manages the library. FTA could utilize one of its University Transit Center partners like Clemson's National Center for Transportation Cybersecurity and Resiliency or MTI's National Transportation Security Center.

Recommendation 7: Develop and Fund Cybersecurity Research Topics

Background and Subcommittee Findings

The cybersecurity space is rapidly evolving, and research will continuously be needed on the most recent advancements. The Subcommittee discussed potential research topics, such as cybersecurity insurance, which MTI has begun to research and fund.[18] Cybersecurity insurance is becoming more expensive and more difficult to obtain for many reasons:

- Cybersecurity attacks are becoming more common and more sophisticated.
- Insurance companies are tightening underwriting guidelines to exclude the transit industry and exiting the cyber insurance market altogether.

[18] Mineta Consortium for Equitable, Efficient, and Sustainable Transportation. Understanding the Current Transit Investment in Cybersecurity. December, 2023. https://transweb.sjsu.edu/mceest/research/utc/Understanding-Current-Transit-Investment-Cybersecurity

- Insurance companies are charging more for the same coverage.
- Insurance companies are requiring more action from the agency or its vendors before offering them coverage.

Many large agencies are choosing to self-insure because of these difficulties, while small- and medium-sized agencies are choosing to not purchase insurance. The Subcommittee found that cybersecurity insurance is becoming increasingly difficult for even large agencies to obtain.

Implementation Suggestions

1. Develop research topics.

The Subcommittee recommends FTA continuously develops research topics. The research topics will evolve over time as the cybersecurity field advances and as new products and ideas are created and become available. The Subcommittee discussed insurance being an immediate research need since it's becoming more expensive and more difficult to obtain as the market is evolving. Additional needs can come from APTA who continuously perform cybersecurity research, especially as it pertains to standards; Transit Cooperative Research Program (TCRP) research recommendations; or from the Transportation Research Board (TRB), like ARM10: Standing Subcommittee on Passenger Rail Transportation, ARM40: Standing Subcommittee on Freight Rail Transportation, or AP080: Standing Subcommittee on Transit Safety and Security.

2. Perform or fund cybersecurity research.

The Subcommittee recommends that FTA either funds or conducts the cybersecurity research developed. By funding or performing the research, FTA can ensure there is a transit component included in the cybersecurity research. The funding for this research could come in the form of a challenge that results in a threat and vulnerability assessment.

3. Publish and promote the research.

The Subcommittee recommends that FTA publishes its research and makes it freely available to the public. The Subcommittee, when discussing cybersecurity insurance, feels that these research documents should cover topics like base requirements for obtaining insurance and how and where to purchase insurance, and inform individual agencies about the adequacy of their cybersecurity investments as compared with their peers.

Conclusion

There is growing concern for public transit agencies about the risk of cyberattacks, as control and management systems become increasingly connected and dependent on IT and OT systems. The Subcommittee found that FTA can help all agencies, especially small- and medium-sized agencies, improve their cybersecurity hygiene. To accomplish this, FTA should clarify and formalize its cybersecurity role; summarize existing guidelines, recommendations, and tools for transit agencies; and create new guidelines, recommendations, and tools for these agencies. These recommendations should

be written so that they are easy for an agency to implement, since many of the smaller agencies do not have robust cybersecurity resources.