Project 2405 | April 2025

Does the Transit Industry Understand the Risks of Cybersecurity and are the Risks Being Appropriately Prioritized?

Scott Belcher, JD, MPP
Terri Belcher
James Grimes
Lusa Holmstrom
Andy Souders

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 Emerging, Efficient, and Safe Transportation (MCEEST) funded by the U.S. Department of Transportation, the California State University Transportation Consortium (CSUTC) funded by the State of California through Senate Bill 1 and the Climate Change and Extreme Events Training and Research (CCEETR) Program funded by the Federal Railroad Administration. 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 Development

To ensure the efficient movement of people and goods, we must prepare the next generation of skilled transportation professionals who can lead a thriving, forward-thinking transportation industry for a more connected world. 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.

Disclaimer

The contents of this report reflect the views of the authors, who are responsible for the facts and accuracy of the information presented herein. This document is disseminated in the interest of information exchange. MTI's research is funded, partially or entirely, by grants from the U.S. Department of Transportation, the U.S. Department of Homeland Security, the California Department of Transportation, and the California State University Office of the Chancellor, whom assume no liability for the contents or use thereof. This report does not constitute a standard specification, design standard, or regulation.

Report 25-04

Does the Transit Industry Understand the Risks of Cybersecurity and are the Risks Being Appropriately Prioritized?

Scott Belcher, JD, MPP

Terri Belcher

James Grimes

Lusa Holmstrom

Andy Souders

April 2025

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.
25-04

2. Government Accession No.

3. Recipient's Catalog No.

4. Title and Subtitle
Does the Transit Industry Understand the Risks of Cybersecurity and are the Risks Being Appropriately Prioritized?

5. Report Date
April 2025

6. Performing Organization Code

7. Authors
Scott F Belcher – 0000-0002-5843-1538
Terri Belcher - https://orcid.org/0000-0002-9355-4357
James Grimes - https://orcid.org/0009-0001-5546-4027
Lusa Holmstrom – https://orcid.org/0009-0002-2925-9457
Andy Souders - 0009-0003-4912-0070

8. Performing Organization Report
CA-MTI-2405

9. Performing Organization Name and Address
Mineta Transportation Institute
College of Business
San José State University
San José, CA 95192-0219

10. Work Unit No.

11. Contract or Grant No.
69A3551747127

12. Sponsoring Agency Name and Address
U.S. Department of Transportation
Office of the Assistant Secretary for Research and Technology
University Transportation Centers Program
1200 New Jersey Avenue, SE
Washington, DC 20590

13. Type of Report and Period Covered

14. Sponsoring Agency Code

15. Supplemental Notes
10.31979/mti.2025.2405

16. Abstract

The intent of this study is to assess the readiness, resourcing, and capabilities of public transit agencies to detect, identify, be protected from, respond to, and recover from cybersecurity vulnerabilities and threats. This study is an update of the 2020 Mineta Transportation Institute (MTI) study, "Is the Transit Industry Prepared for the Cyber Revolution? Policy Recommendations to Enhance Surface Transit Cyber Preparedness." In the previous study, the authors found that the transit industry was ill-prepared for cybersecurity attacks. Unfortunately, after four years and the development of new, and often free, resources, the situation has not markedly improved. In fact, this survey, which included a larger number of small rural transit agencies, shows that they lag far behind their larger peers. The increasing sophistication of cybercriminals, in combination with a greater reliance on technology within the transit industry, puts the industry at greater risk than in 2020. This study reviews and updates the state of best cybersecurity practices in public surface transit; outlines U.S. public surface transit operators' cybersecurity operations and the resources available to them; reviews U.S. policy on cybersecurity in public surface transportation; and provides policy recommendations that address gaps or identify issues for Congress, the Executive Branch, public surface transit agencies, and their associations and other supporting organizations. Research methods include an online survey and oral interviews with public surface transit agencies in the United States as well as oral interviews with members of the Executive Branch (e.g., the U.S. Department of Transportation, the U.S. Department of Homeland Security), as well as research of literature published in periodicals. There is an exponentially expanding gap between the cybersecurity preparedness that should exist and the growing threats from increased reliance on technology and the opportunities by malicious actors. This research provides information that can be used to help close that gap.

17. Key Words
Cybersecurity, enterprise risk management, policy, security, transit.

18. Distribution Statement
No restrictions. This document is available to the public through The National Technical Information Service, Springfield, VA 22161.

19. Security Classif. (of this report)
Unclassified

20. Security Classif. (of this page)
Unclassified

21. No. of Pages
125

22. Price

DOI: 10.31979/mti.2025.2405

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/2405

Acknowledgements

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

The American Public Transportation Association (APTA), including Paul Skoutelas, President and CEO; David Carol, Chief Operating Officer; Polly Hanson, Senior Director of Security, Risk and Emergency Management; and the APTA team for their ongoing support and guidance;

The Community Transportation Association of America (CTAA), including Scott Bogren, Executive Director; Loreal Lance, Director, Member Services, Business Development, and Events; and the CTAA team for their ongoing support and guidance;

The American Association of State Highway Officials (AASHTO), including James Tyman, Executive Director; Rebecca Anger, Manager for Transit Policy and Technical Assistance; and the rest of the AASHTO team for their ongoing support;

Editing Press for editorial services; and Mineta Transportation Institute (MTI) staff, including Karen Philbrick, PhD, Executive Director; Hilary Nixon, PhD, Deputy Executive Director; and the rest of the MTI team for their ongoing support.

CONTENTS

LIST OF FIGURES

Executive Summary

Information abounds for public transit agencies to develop their own cybersecurity preparedness programs; however, without regulatory requirements and resources, many transit agencies will not likely put in place basic cybersecurity resilience and response programs. Small and rural agencies, in particular, lack the resources and technical expertise, do not prioritize cybersecurity, or do not believe they are targets. There is a significant amount of useful, effective, and free information available to assist transit agencies in implementing a cybersecurity program: they can use the National Institute of Standards and Technology (NIST) cybersecurity assessment framework and implementation guides as well as guidance from multiple federal agencies, associations, private industries, and others. However, despite these resources, far too many agencies have not implemented adequate cybersecurity measures and are not prepared to respond to a cyber incident, a finding that has changed little over the past four years.

For this report, the authors conducted a digital survey to understand each agency's level of cybersecurity preparedness as well as dozens of in-person and phone interviews. This survey is similar to the one used in the 2020 study, "Is the Transit Industry Prepared for the Cyber Revolution? Policy Recommendations to Enhance Surface Transit Cyber Preparedness"[1] (hereafter, 2020 MTI Study), allowing for a comparison across the two time periods. One of the most startling statistics to come from this work is that 90% of the agencies that responded to the 2024 survey report that they did not have a cybersecurity incident in the past year. Data and research from other industries suggest that the survey respondents under reported the number of cybersecurity incidents.

U.S. Experiences its Largest Cybersecurity Hack

> As the authors were finishing up this report, news broke of a hack against U.S. telecommunications providers by the Chinese hacking group dubbed Salt Typhoon. This hack compromised at least eight of America's telecom networks and is being called the largest U.S. hack to date. The intruders stole the call-record metadata on a "large number" of Americans as well as wiretap requests made by law enforcement agencies. News began trickling out in September, but government officials did not confirm reports until weeks later and only began briefing members of Congress in December. As this report concluded, this hack had still not been contained. Why does this matter? The U.S. telecommunications industry is among the most technologically sophisticated industries, is well resourced, and takes cybersecurity very

[1] Scott Belcher, Terri Belcher, Eric Greenwald, and Brandon Thomas, "Is the Transit Industry Prepared for the Cyber Revolution? Policy Recommendations to Enhance Surface Transit Cyber Preparedness," Mineta Transportation. DOI:10.31979/mti.2020.1939

> seriously. Yet, they had a foreign cybercriminal in their networks since 2022 before it was discovered and it became a national security crisis.

The problem may be that cybersecurity is still not widely viewed as a critical issue among public transit leadership. Unfortunately, the cybersecurity incidents that have occurred have not spurred the broad scale response that one might expect. Both the reporting of and accountability for cybersecurity attacks remain murky given the current regulatory environment. There is an exponentially expanding gap between the cybersecurity preparedness that should exist and the growing threats from increased reliance on technology and opportunities by malicious actors.

The report concludes with a series of policy recommendations intended to engage Congress, the Executive Branch, transit agencies, associations, and other supporting organizations to find ways to establish minimal cybersecurity requirements, provide funding to implement them, and inform agency leadership about the need for action.[2]

As a result of the interviews the authors conducted, numerous interviewees suggested that a brief outline or one pager would be helpful to share with their boards and leadership. Set forth below are highlights for Board Members, Executive Leadership, and Technology Professionals.

Key Take-Aways for Board Members

- A cybersecurity breach can impact the financial viability, operational capability, and reputation of the organization.

- Every agency is at risk of a cybersecurity breach, regardless of size.

- Cybersecurity is an enterprise risk management issue, not solely a technology issue, and the Board should be regularly briefed on how the organization is managing all enterprise risks, including cybersecurity. As such, cybersecurity should be part of every board's agenda.

- The board has a fiduciary obligation to ensure the organization is cognizant of the threat posed by a cybersecurity breach, is aware of the organization's vulnerabilities, and has a plan to address them.

- The board should ensure that the organization has cybersecurity insurance or is capable of self-insuring against a cybersecurity breach.

[2] Richard Forno, "What is Salt Typhoon? A Security Expert Explains the Chinese Hackers and Their Hacks on US Telecommunications Networks," *UMBC Magazine*, December 6, 2024, https://umbc.edu/stories/what-is-salt-typhoon-a-security-expert-explains-the-chinese-hackers-and-their-attack-on-us-telecommunications-networks/.

Key Take-Aways for Executive Leadership

- A cybersecurity breach can impact the financial viability, operational capability, and reputation of the organization.

- Every agency is at risk of a cybersecurity breach, regardless of size.

- Cybersecurity is an enterprise risk management issue, not solely an IT issue.

- Executive leadership has a fiduciary obligation to ensure that the organization is cognizant of the threat posed by a cybersecurity breach, is aware of its vulnerabilities, has internal controls in place to manage them, and keeps the board apprised as part of every board meeting.

- Executive Leadership should encourage collaboration with other agencies through industry trade associations and other supporting organizations to become stronger together in the cybersecurity domain.

- Executive Leadership should ensure that the organization is following the recommendations set forth in the Transportation Security Administration (TSA), *Information Circular IC-2021-01, Enhancing Surface Transportation Cybersecurity TSA Circular for Surface Transportation*, specifically:

    - Designate a Cybersecurity Coordinator

    - Report Cybersecurity Incidents

    - Implement a Cybersecurity Incident Response Plan

    - Perform a Cybersecurity Vulnerability Assessment

- Executive Leadership should ensure that the organization has written cybersecurity policies and procedures in place and is following them.

- Executive Leadership should be aware of the role that their part of the organization must play in preventing and responding to a cybersecurity attack.

- Executive Leadership should ensure that the organization has cybersecurity insurance or is capable of self-insuring against a cybersecurity breach.

- Executive Leadership should be aware of any federal, state, or local cybersecurity requirements impacting the organization and ensure that the organization follows them.

- Executive Leadership should be aware of the cybersecurity resources available to the organization and avail themselves of them as appropriate.

Guidance for Technology Professionals

The objective of cybersecurity is to protect the entire infrastructure of an agency, encompassing both Information Technology (IT) and Operational Technology (OT) environments, from unauthorized access and malicious threats. Cyber resilience assumes that when an agency experiences a cyber event, it can sustain operations and recover rapidly, minimizing downtime and impact on customers. This includes developing effective response strategies and recovery plans to restore functionality and maintain continuity. Cybersecurity preparedness involves implementing proactive measures to identify, protect, and detect vulnerabilities and risks within an agency's infrastructure, including on-premise and cloud systems, agency operated hardware and software, and vendor operated hardware and software. As specifically addressed in the study and reported in Section IV Findings, the authors recommend the following:

Cyber Resilience

- **Cybersecurity Assessments** – Conduct regular cybersecurity assessments of preparedness and resilience to evaluate the Agency's preparedness and recovery capabilities. Use the findings to close critical gaps and drive continuous improvements in prevention, response processes, and recovery plans.

- **Disaster Response Planning and Testing** – Develop and maintain a comprehensive Disaster Response plan and business continuity strategies, and regularly test them through tabletop and partial data recovery exercises, ensuring critical systems and applications can be restored promptly with minimal disruption to operations.

- **Cybersecurity Incident Response (IR) and Testing** – Develop and maintain a comprehensive IR plan that aligns with agency recovery objectives. Integrate IR playbooks with pre-defined actions for various cyber scenarios, ensuring quick mobilization and coordination across teams during incidents and regularly test them through tabletop and partial data recovery exercises.

Cybersecurity Preparedness

- Continuous Employee Cybersecurity Training – Provide ongoing, role-specific training programs focused on phishing detection, secure practices, and awareness of emerging threats, ensuring personnel are equipped to recognize and respond to security risks.

- Comprehensive Log Management – Implement centralized logging mechanisms that aggregate, correlate, and analyze data from various sources in real time. Maintain backup protocols to secure essential logs for forensic investigations and compliance requirements.

- Vendor Management and Assessment – Execute continuous security assessments of third-party vendors, focusing on their compliance with security standards and adherence to risk management policies. Incorporate third-party risk management frameworks to evaluate vendor security postures systematically. Review existing contracts to ensure that vendors are maintaining adequate cybersecurity hygiene and address cases in which they are not. Ensure that all new contracts have cybersecurity provisions that require an appropriate level of cybersecurity hygiene and protections for the agency.

Although it was not specifically asked as part of the survey, the authors recommend the additional Cybersecurity Preparedness objectives to further reduce risk:

- **Multi-Factor Authentication (MFA)** – Enforce MFA for all critical systems, particularly those with privileged access, to mitigate risks associated with unauthorized access and credential theft.

- **Patch Management and Vulnerability Scanning** – Establish automated patch management to ensure timely application of patches and updates, addressing known vulnerabilities, and reducing the exploitable surface. Conduct regular internal and external vulnerability scans using advanced tools and manual analysis to identify and prioritize remediation actions.

- **Penetration Testing and Adversarial Simulation** – Implement a continuous penetration testing program that simulates real-world attack scenarios instead of a "one and done" annual approach. Try to mimic adversary tactics, techniques, and procedures to identify potential weaknesses in response protocols.

- **Network Segmentation of IT and OT Environments** – Architect and implement strict segmentation protocols within and between IT and OT networks to contain threats, prevent lateral movement, and safeguard critical operational assets.

- **Advanced Anti-Virus and Endpoint Detection and Response (EDR)** – Deploy anti-virus solutions with heuristic and behavioral capabilities to detect and prevent sophisticated threats. Integrate EDR tools to provide continuous endpoint monitoring, enabling proactive threat hunting and automated response to malicious activities.

- **Principle of Least Privilege (PoLP)** – Enforce PoLP by rigorously controlling access rights, ensuring users, systems, and applications only have permissions necessary for their functions, reducing attack vectors.

While these best practices are applicable to all agencies, the authors recognize that without additional funding and a government mandate, they might not all be attainable by small agencies.

1. Introduction

In 2020, the Mineta Transportation Institute (MTI) published an assessment of the transit industry's capability to prepare for and respond to a cybersecurity attack. This report, "Is the Transit Industry Prepared for the Cyber Revolution? Policy Recommendations to Enhance Surface Transit Cyber Preparedness"[3] (hereafter, *2020 MTI Study*), was based on a detailed survey, interviews, and thorough research. The *2020 MTI Study* concluded that much of the transit industry was not prepared for the wave of cybersecurity attacks and that a significant number of agencies did not have basic protections in place. Since that time, the federal government, states, supporting organizations, and the private sector have actively promoted the importance of putting in place cybersecurity protections and have made available multiple resources to aid transit agencies.

For this study, the authors replicated the study methodology of the *2020 MTI Study* to assess the progress that had been made since 2020. Based on the 2024 survey responses, interviews, and literature review, it is apparent that while progress has been made by many of the larger transit agencies, much work still needs to be done by rural, small-, and medium-sized agencies.

Many Transit Agencies Do Not Appreciate the Risks Posed by Cybersecurity

> Many agencies do not have sufficient resources to address cybersecurity issues, do not view cybersecurity as a sufficient priority to warrant moving resources away from other priorities, believe they have necessary protections in place, or think that they are too small to be targets.

Unfortunately, neither the increase in the number of attacks and their severity, nor the limits on the ability to insure against them, has spurred the response one might expect. Although both reporting and accountability by some agencies have improved, to whom to report, what must be reported, and when a report must be filed remains very complex given the multiple oversight bodies. There are also large gaps between cybersecurity preparedness and cybersecurity resilience, different risks posed by Information Technology (IT) and Operational Technology (OT), greater connectivity, and new risks posed by bots, artificial intelligence, and cyber-attacks as a service.

The report concludes with a series of policy recommendations intended to engage Congress, the Executive Branch, transit agencies, associations, and supporting organizations to find ways to continue to direct, fund, and educate transit agency leadership to take cybersecurity threats seriously and allocate the necessary resources to minimize the risks of a breach and improve an agency's ability to respond.

[3] Belcher, Belcher, Greenwald, and Thomas, "Is the Transit Industry Prepared for the Cyber Revolution?"

1.1 Public Transportation Overview

For this study, public transportation is defined as urban and rural bus systems, paratransit, bus-rapid transit (BRT), water-borne services, subways, light rail, streetcars and other urban rail networks, and passenger rail. This distribution of transit services is shown in Figure 1.

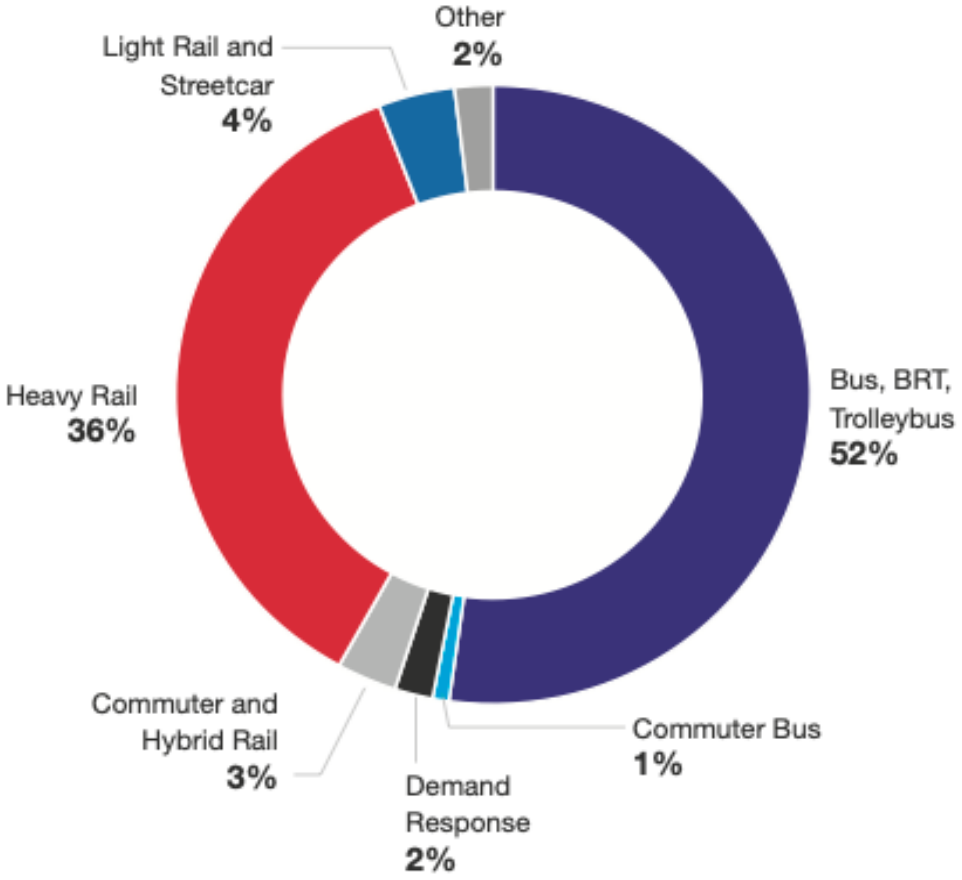
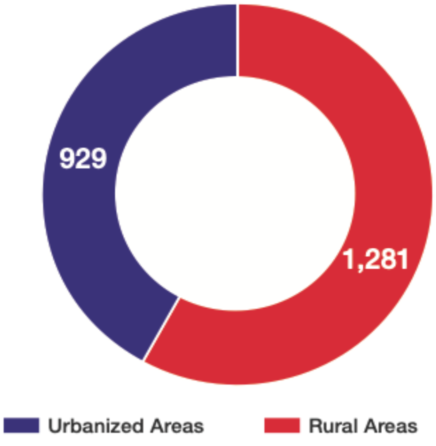


Figure 1. Share of Unlinked Passenger Trips by Mode, 2021[4]

The American Public Transportation Association (APTA) produces an annual fact book based on data from the Federal Transit Administration's (FTA) National Transit Database (NTD). The *2023 Public Transportation Fact Book* reports that approximately 6,800 organizations provide public transportation in the United States through the various transit modes shown in Figure 1. Of this total, an estimated 4,580 are public nonprofit providers. Systems operating in urban and rural areas that receive grant money from the Federal Transit Administration's (FTA) Urbanized Area

[4] Matthew Dickens, *2023 Public Transportation Fact Book*, 74th ed. (American Public Transportation Association (APTA), March 2024), 10, https://www.apta.com/wp-content/uploads/APTA-2023-Public-Transportation-Fact-Book.pdf.

Formula Grant Program (5307)[5] or the Formula Grants for Rural Areas Program (5311)[6] are required to report to the NTD as full, reduced, or rural systems. The NTD is the primary source for information and statistics on transit systems in the United States. The U.S. Congress requires the NTD to collect financial and service information annually from public transportation agencies that receive benefits from FTA grants.[7] In 2021, 2,210 transit systems reported to the NTD, of which 1,281 were in rural areas and 929 were in urbanized areas (these numbers are almost the same as the *MTI 2020 Study*).



SOURCE: NATIONAL TRANSIT DATABASE

Figure 2. NTD Reporting Transit Systems by Area Type[8]

Although rural agencies comprise more than 57% of the transit agencies reporting to the NTD, these agencies provide less than 2%[9] of the total unlinked passenger trips taken. Unlinked passenger trips are an industry method that tracks ridership by counting each time a passenger boards a transit vehicle, including transfers. Rural transit trips, while not large in numbers, are important trips because they can be the primary method of transportation for people who cannot or do not drive.

Large transit agencies handle most of the public transit trips in the United States, and the largest agencies receive the largest share of federal resources. Of the 2,210 agencies that reported to the NTD in 2021, nine have operating expenses that exceed a billion dollars a year. These nine agencies are in the largest metropolitan cities in the United States and handled 4.25 billion

[5] "Urbanized Area Formula Grants – 5307," Federal Transit Administration (FTA), accessed August 2, 2024, https://www.transit.dot.gov/funding/grants/urbanized-area-formula-grants-5307.

[6] "Formula Grants for Rural Areas – 5311," FTA, accessed August 2, 2024, https://www.transit.dot.gov/rural-formula-grants-5311.

[7] *2021 National Transit Summaries & Trends* (FTA, December 2022), 2, https://www.transit.dot.gov/sites/fta.dot.gov/files/2022-11/2021%20National%20Transit%20Summaries%20and%20Trends_1-1.pdf.

[8] Dickens, *2023 Public Transportation Fact Book*, 7.

[9] *2021 National Transit Summaries & Trends*, 26, 67.

unlinked passenger trips in 2021, more than 60% of the 7.1 billion total trips in 2021. It is tempting, because of these numbers, to focus cybersecurity efforts on the very largest agencies. While this approach may provide protection to the largest number of riders, it fails to address the other 2,200 transit agencies that also report to the NTD and the 4,000 transit agencies that do not report and are still the targets of cybersecurity attacks.

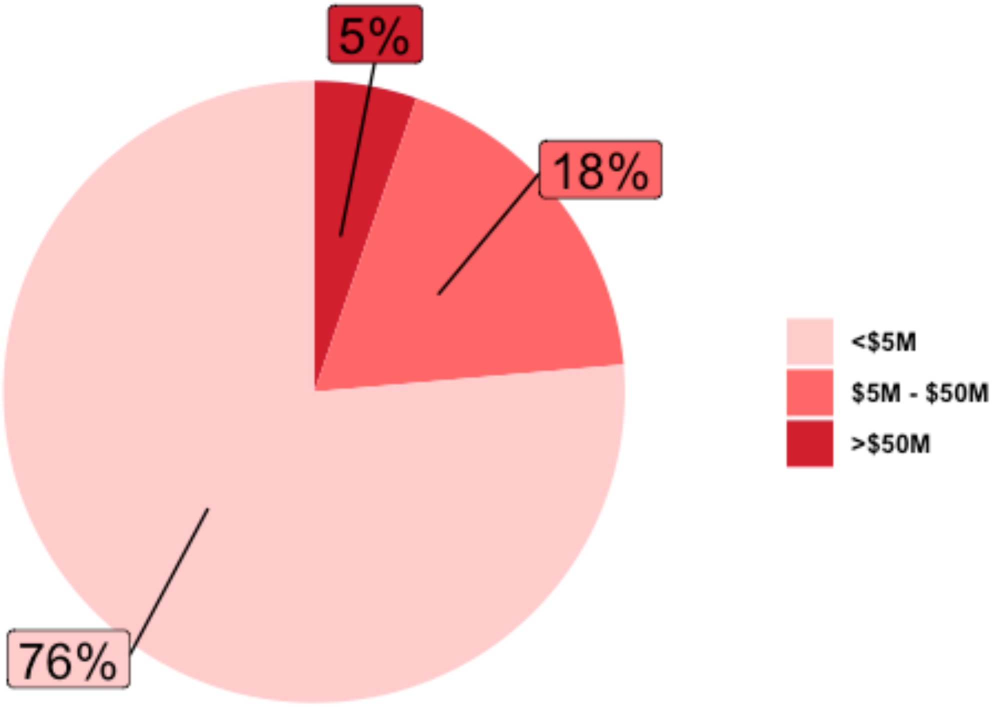


Figure 3. Industry-Wide Transit Agency Annual Operating Expenses (2022)[10]

As seen in Figure 3, 76% of the transit agencies reporting to the NTD have less than $5 million in annual operating expenses, which means most targets in the transit sector are small agencies with limited resources. The problem facing small- to medium-sized agencies is complex; smaller agencies for the most part do not have the staff or budget to defend against cyber-attacks; they face highly sophisticated cyber criminals that are constantly changing their attack methods and looking for new targets. CrowdStrike summed this up in a blog posting from 2023, noting that small- and medium-sized businesses are more frequent targets for cybercrime than large businesses and that as larger businesses have become better at defending themselves, criminals have turned to small- and medium-sized businesses.[11]

[10] "2022 Annual Database Operating Expenses," FTA, last updated April 12, 2024, accessed August 6, 2024, https://www.transit.dot.gov/ntd/data-product/2022-annual-database-operating-expenses.

[11] Joe Faulhaber and Brad Moon, "Small Business Cyber Attack Analysis: Most Targeted SMB Sectors and Key Prevention Tips," CrowdStrike, January 30, 2023, accessed February 11, 2024, https://www.crowdstrike.com/en-us/blog/small-business-cyberattack-analysis-most-targeted-smb-sectors/.

Due to the COVID pandemic, public transportation ridership in report year 2021 was much lower than in previous years. Public transportation provided 4.49 billion unlinked passenger trips in report year 2021, a decrease of 25% compared to 2020[12] (Figure 4).

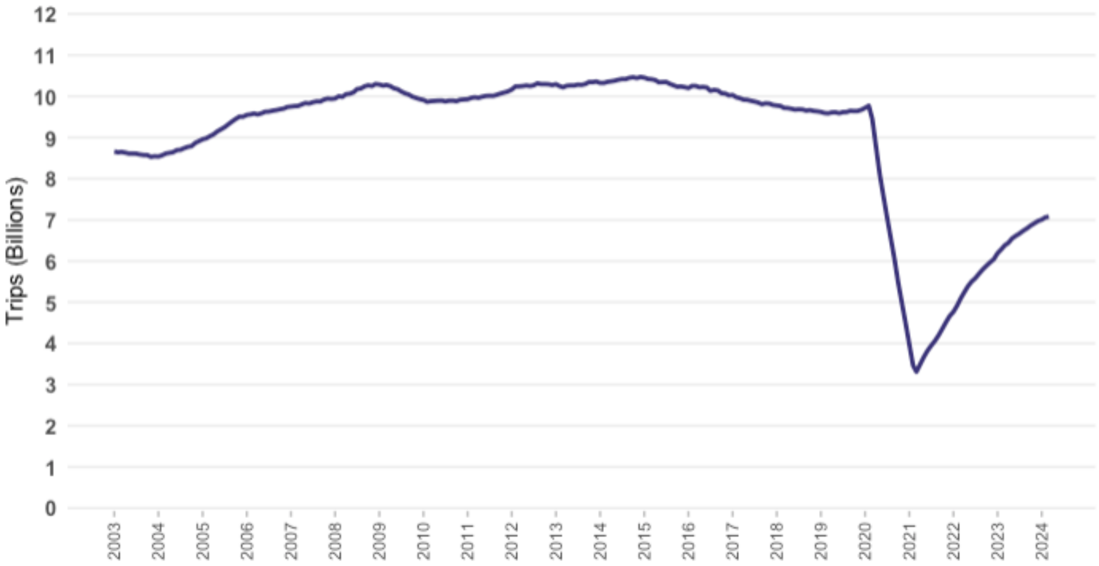


Figure 4. Rolling 12-month Ridership, 2003–2024[13]

The good news for public transit is that, since 2021, public transportation ridership has rebounded. Although ridership has not returned to pre-pandemic levels, some systems are close to full recovery, though many still lag. Overall, APTA reports that transit ridership has recovered to 79% of pre-pandemic levels.[14] Buses have seen a faster recovery than rail, primarily driven by demographic differences in ridership; a larger proportion of rail riders work office jobs which are easier to perform remotely. Smaller cities have also seen better transit recovery than larger ones.[15]

[12] Dickens, *2023 Public Transportation Fact Book*, 10.

[13] "May 2024 Raw Monthly Ridership," FTA, July 2024, accessed July 22, 2024, https://www.transit.dot.gov/ntd/data-product/monthly-module-raw-data-release.

[14] Jared Bonia and Matthew Dickens, "APTA Public Transportation Ridership Update," April 2024, 4, https://www.apta.com/wp-content/uploads/APTA-POLICY-BRIEF-Transit-Ridership-04.01.2024.pdf.

[15] Bonia and Dickens, "APTA Public Transit Ridership Update," 3.

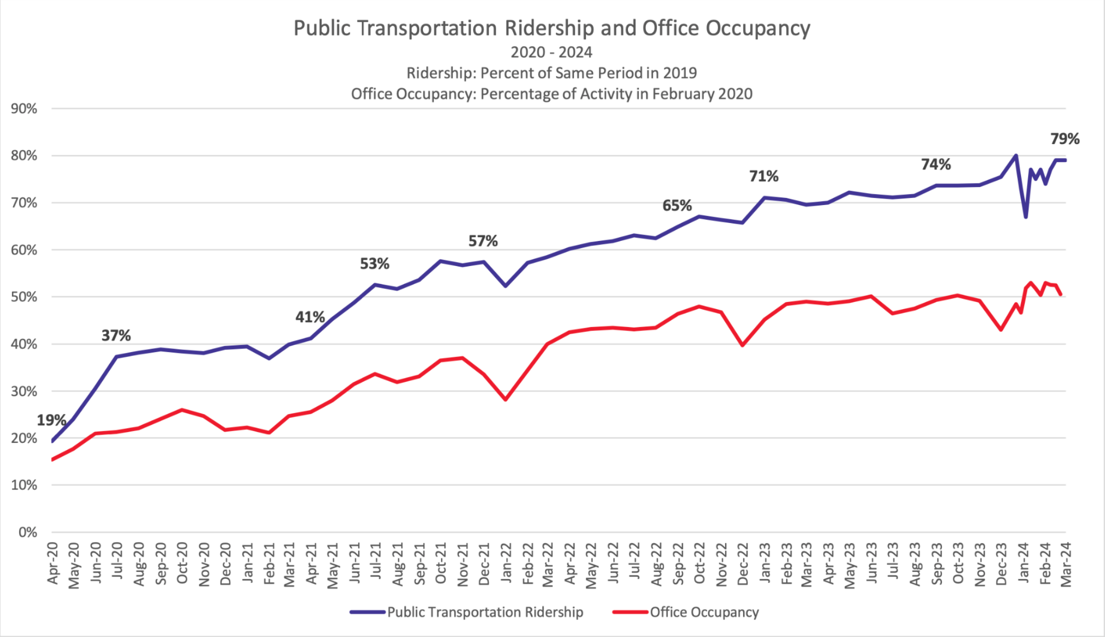


Figure 5. Ridership and Office Occupancy, April 2020 to March 2024[16]

The COVID pandemic brought with it a host of cybersecurity risks. Many offices and systems were not prepared for broad-scale work-from-home employees, new digital technologies attempting to provide better services, or the move from fixed bus route to on-demand services. As more systems adapt and resources continue to be digitized and become more connected, an increasing number of opportunities arise for malicious actors to disrupt operations on a massive and potentially catastrophic scale.

Even before the pandemic, the move to a more digitally connected environment raised concerns among industry leaders. Back in 2018, APTA Board Chair Nathaniel P. Ford Sr., CEO of the Jacksonville Transportation Authority, was quoted in an interview: "As we expand our use of technologies, such as data-sharing and driverless vehicles, the threat keeps growing. Public transportation agencies of all sizes and at all locations are at risk. This is why I have made cybersecurity one of my top priorities."[17] Jeff Nelson, the CEO and General Manager of Rock Island County Metropolitan Mass Transit District, Quad Cities (QC) MetroLINK, and the APTA Board Chair in 2019–2020 after Nathaniel Ford, made the use of technology in the transit industry and its impact on cybersecurity risk a top priority.

There are several issues affecting transit agencies that exacerbate their cybersecurity exposure and will continue to add pressure for oversight from both federal and state entities. The first area of concern is data. Transit agencies today continuously generate increasingly large volumes of data.

[16] Bonia and Dickens, "APTA Public Transit Ridership Update," 4.

[17] Alex Roman, "Q&A with APTA Chair and JTA CEO Nathaniel P. Ford Sr.," *METRO*, February 12, 2018, accessed October 14, 2024, https://www.metro-magazine.com/10007328/qa-with-apta-chair-and-jta-ceo-nathaniel-p-ford-sr.

However, many agencies have systems in which their data remains siloed and is often not integrated with other internal or—more importantly—external systems.

In many instances, this fragmented architecture has worked to transit agencies' advantage as it has hampered hackers' efforts to access transit data. However, as more systems, processes, and applications move online both within an organization and are integrated with other public and private organizations, there is greater risk. Data at risk include employee information and operational data, as well as customer and financial data. As the connected nature of this data grows, so too will the risks that malicious actors may target that data for theft or disruption.

The Ability to Access Transit Data in New Ways Creates New Opportunities for Cybersecurity Criminals

> In 2024, the Transit Authority of Northern Kentucky was the victim of a ransomware attack by the Akira Group. The Akira Group accessed a range of sensitive data, including employee personal information, confidential agreements, contracts, incident reports, and some customer data. Akira's tactics include unauthorized access to VPNs, credential theft, and lateral movement to deploy the ransomware.[19]

The increased use of technology in the transit industry has also increased the potential for disruption to public transit activities. Vehicle connectivity is incredibly broad. Numerous technologies are already in public transit vehicles; they include global positioning systems (GPS), Wi-Fi, cellular, radio, dedicated short range communications (DSRC), and connected vehicle systems. These technologies allow transit agencies to send data back and forth, in real time, between their vehicles and the command center, the cloud, other vehicles, and the internet.

Vehicle connectivity is not only making the data integrated and systemically accessible, but it is also making the data from the operation of the vehicle accessible in digital form. The ability for a malicious actor, with the right access and tools, to alter the operation of vehicles has become technically more feasible as more vehicles are digitally connected to each other.

Transit agencies must take cyber threats seriously and invest in both cybersecurity preparedness and resilience. Current guidance and support for transit agencies exists in many forms and in many locations, but it requires transit agencies to take a more active role and ensure agency-wide understanding and compliance. There are few regulations, but, in many cases, best practices do exist. Transit agencies that act now to protect themselves will not only be safer from the disruption

[19] "Ransomware Disrupts the Transit Authority of Northern Kentucky," Halcyon, August 19, 2024, accessed August 21, 2024, https://www.halcyon.ai/attacks/ransomware-attack-disrupts-northern-kentucky-transit-authority-tank.

of cybersecurity threats, they will also be better positioned to meet and influence federal, state, and other regulatory activities.

The intent of this report is to make the case for mandatory minimum cybersecurity standards, federal investment to help agencies meet these standards, and additional support to help agencies stay abreast of the everchanging threat environment.

1.2 Report Organization

Section I of the report introduces the transit industry and the growing risks that cybersecurity presents. Section II provides a summary of the methods used to research the subject matter and compile this report. Section III discusses transit agency's cybersecurity vulnerabilities and risks. Section IV provides a review of the guidance and resources available to transit agencies. Section V explores the findings from this study. Section VI provides policy recommendations to better support cybersecurity preparedness and resilience among public transit agencies.

2. Methodology

This study started with the *2020 MTI Study* as its base and updated its analysis, findings, and recommendations based on the 2024 survey responses, interviews, and additional research. As with the *2020 MTI Study*, the authors employed a multi-method approach to research and evaluate the status of public transit agencies' cyber preparedness and resilience and to develop policy recommendations to improve their posture. The study focused on public surface-transit agencies that receive funding from the FTA and operate in the United States.[20]

Literature Review: The authors reviewed literature on physical and digital cybersecurity strategies in transit as well as other industries and applied key findings from this review to develop digital surveys and policy recommendations. The authors supplemented the literature review with an internet search of recent cyber incidents and innovative and emerging trends in cybersecurity. The authors attended and presented on cybersecurity at several relevant sessions at conferences sponsored by APTA, AASHTO, CTAA, ITS America, and the Transportation Research Board (TRB).

Expert Interviews: For this study, the interviews were conducted by Scott Belcher, Andy Souders, and James Grimes. The first group focused on transit agencies and included interviews with transit chief executives, chief security officers, and IT professionals. These interviews gathered data from public transit operations and were representative of the size, geographic scope, and diverse nature of the nation's public transit operators. The second group focused on interviews with individuals working for companies supporting transit agencies (e.g., vendors, trade associations, cybersecurity professionals). The third group focused on interviews with government officials. These interviews included representatives of the U.S. Department of Transportation (DOT), the FTA, the U.S. Department of Homeland Security (DHS), and the White House Office of Science and Technology Policy (OSTP).

Digital Survey: Based on the information gathered in the literature review and the oral interviews, the authors updated a digital survey from the *2020 MTI Study.* The survey was sent directly to the CEOs of the approximately 300 active APTA public transit members. AASHTO and CTAA sent the survey through their organizations' respective newsletters. Survey responses were compared to NTD data. The authors followed up on the original survey requests via email and telephone. From these organizations, the authors received 86 responses. Two responses were removed because they were non-US transit operators, and three responses were removed because they came from organizations which do not have transit operations. Four organizations submitted two responses, resulting in a total of 78 responses. The authors followed up multiple times with organizations whose responses were incomplete via a supplementary survey, email, and phone interviews.

[20] Private agencies and agencies that serve other countries were considered out of the study's scope. Only agencies that provide surface transit were considered.

Altogether, the agencies that responded to the survey serve over 72 million people—roughly a fifth of the entire population of the United States. Of the 78 agencies, 26 (one third of respondents) are considered rural, having lower population densities and different operating models.[21] Rural agencies are also subject to fewer FTA reporting requirements. This is a large increase from the *2020 MTI Study*, where only five rural agencies participated. Nearly 60% of public transit agencies in the NTD are rural, but they comprise less than 2% of the transit trips in the United States.[22] A more detailed review of the populations that survey's respondents serve shows a broad distribution (Figure 6).

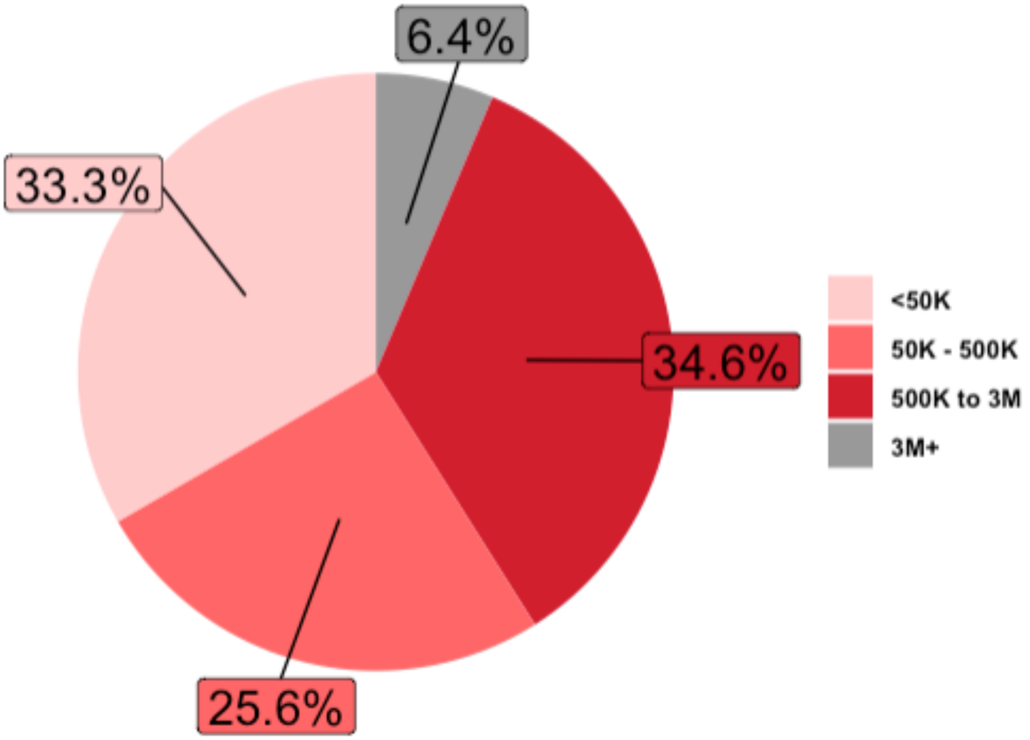


Figure 6. Population Served of Survey Respondents[23]

The survey netted a similarly broad distribution with respect to the organizational size of the responding entities. Agencies ranged in size from less than $500,000 to more than $2 billion in operating expenses. Of the responses received, 34% had annual operating budgets of less than $5 million, 29% had operating budgets between $5 and $50 million, and 38% had budgets above

[21] Sohail Husain, "Rural Transportation Challenges: Stakeholder Perspectives," Eno Center for Transportation, March 22, 2024, accessed October 9, 2024, https://enotrans.org/article/rural-transportation-challenges-stakeholder-perspectives/.

[22] *2021 National Transit Summaries & Trends*, 26, 67.

[23] *2022 Annual Database Agency Information* (FTA, last updated July 17, 2024), accessed August 6, 2024, https://www.transit.dot.gov/ntd/data-product/2022-annual-database-agency-information.

$50 million. Where the data identifies differences in survey responses that appear to be based solely on size or on the rural nature of the transit agency, these differences are highlighted for the reader.

Policy Recommendations: The authors identified four focus areas for recommendations: Congress, Executive Branch, transit agencies, and their trade associations and other supporting organizations.

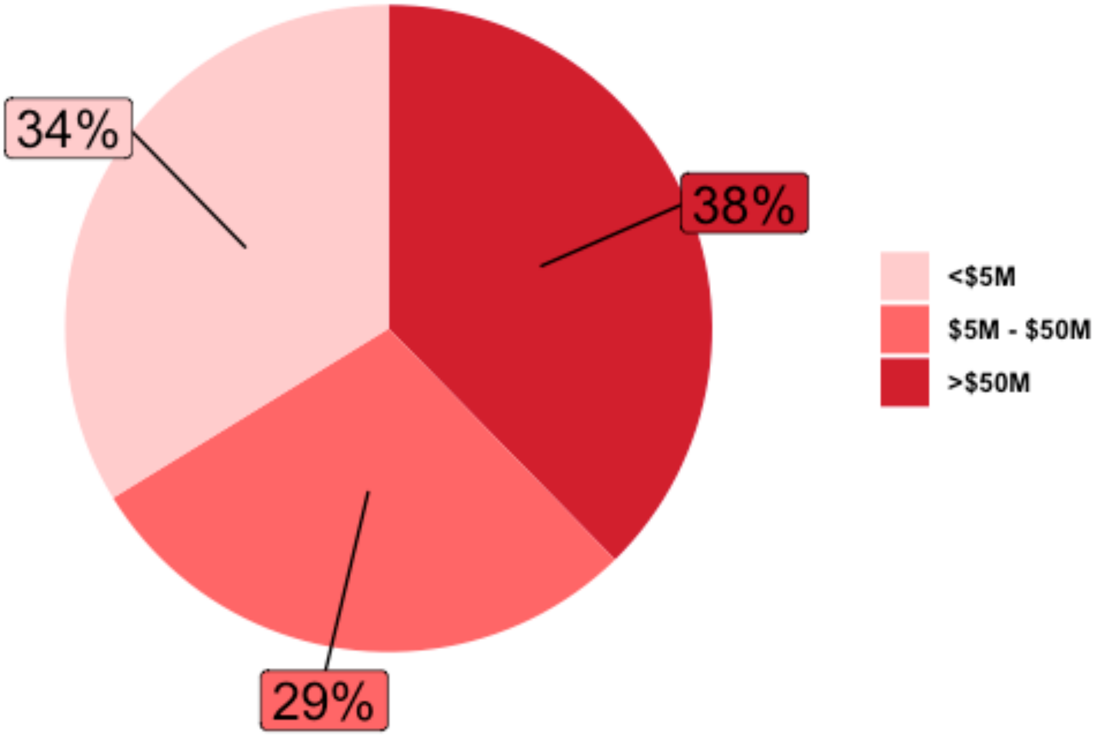


Figure 7. Size of Agencies that Responded to 2024 Survey

Study's Limitations: The intent of this study is to update the findings from the *2020 MTI Study* with the results from the survey and interviews conducted in 2024. The authors assessed the readiness, resources, structure, and governance of public transit agencies to identify, protect from, detect, respond to, and recover from cybersecurity vulnerabilities and threats.[24]

In this report, the authors focused on identifying actionable items that transit agencies could take to improve cybersecurity in a manner that is agnostic to the specific technologies that those agencies employ. Although the authors examined the threats currently facing transit agencies, they

[24] These five actions, along with governance, are the six key functions that are the backbone for the Cybersecurity Framework established by the National Institute of Standards and Technology (originally established in February 2014).

did not scrutinize threats posed by specific technologies being implemented by many transit agencies.

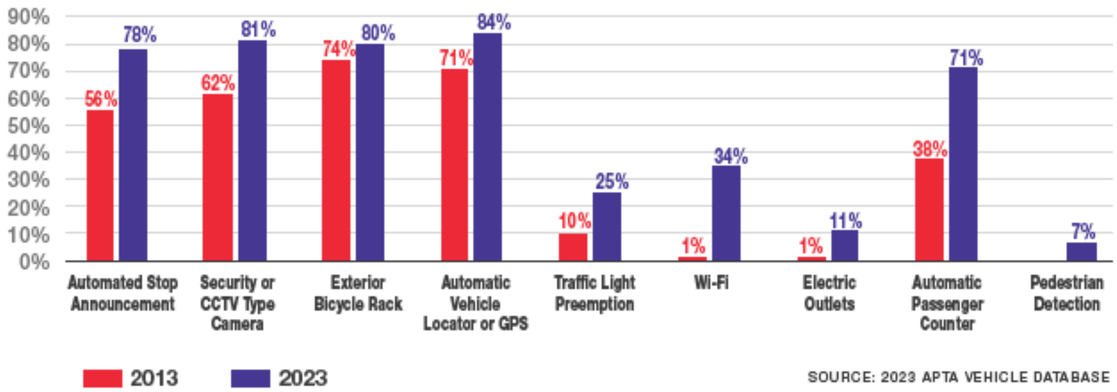
The authors did not assess the internal cybersecurity capabilities of public or private organizations with whom many agencies integrate and/or share data, such as major industry vendors, supporting organizations, and/or federal or state governmental agencies.

Finally, when the *2020 MTI Study* was written, the COVID pandemic was in the midst of spreading across the globe. The transit industry experienced an unprecedented drop in ridership, and the long-term consequences of the pandemic on transit are still unclear.

3. Transit Cybersecurity Risk Profile

Like every facet of society, the use of technology and data in public transit continues to evolve. Each aspect of transit operations is subject to change, whether it is routing, scheduling, or payment. Payment has moved from fare boxes, in which riders inserted cash or coins on the bus, to off-board payment by smartphone and digital wallet. Routing changes that were once exclusively done manually are now considerably improved with modern mapping technology, better software, artificial intelligence, and machine learning. Transit operators can now run real-time route scenarios to optimize their services. Knowing when and where to catch the next bus used to require a series of paper printouts and signs. Today, riders can not only obtain this information on their smartphones, but, in many cases, it will also be updated in real time. Transit service is evolving from a predominantly fixed-route and fixed-schedule system to on-demand.

The modern transit operator collects and maintains an ever-increasing volume of data concerning its operating systems, vehicles, and customers. Public transit vehicles transmit operator communications, bus operations data, live video, and rider internet activity. This data has made public transit more convenient, safer, and more efficient. Automatic passenger counters, centrally aided dispatch, automatic vehicle location software, and real-time bus/train arrival systems have improved transit operations. Similarly, technologies such as traffic signal preemption, dynamic re-routing, bus lane enforcement, and automated driver assist systems have also increased bus and transit system safety and efficiency (Figure 8).



SOURCE: 2023 APTA VEHICLE DATABASE

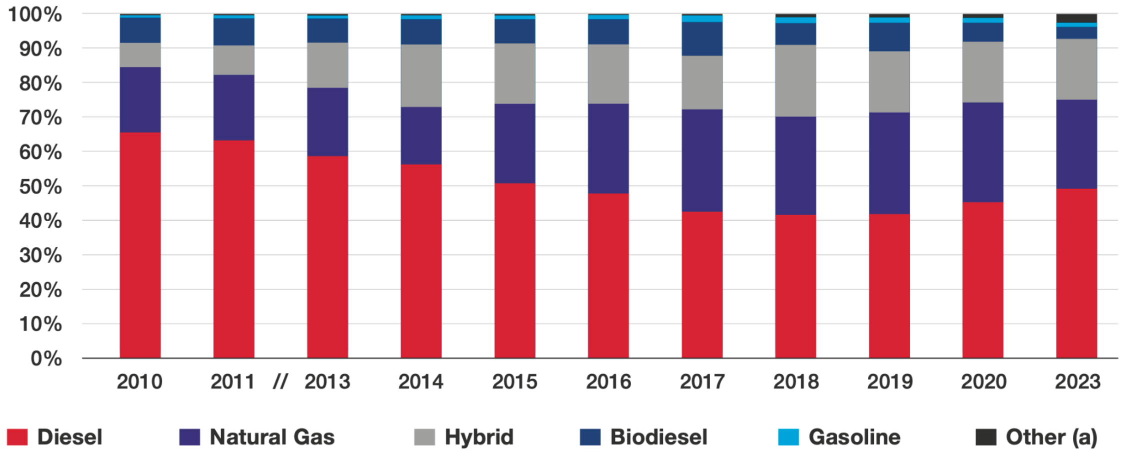
Figure 8. Percentage of Buses with Passenger Equipment, 2013–2023[25]

Transit systems have also become increasingly complex, owing to an ever-increasing use of transportation network companies (TNCs), first- and last-mile Mobility on Demand (MOD) services, mobility-as-a-service (Maas) options, autonomous or near-autonomous vehicles, and micro-mobility integration. Additionally, over the past several years the federal government has pushed transit agencies to adopt alternative fuel sources such as compressed natural gas, electricity,

[25] Dickens, *2023 Public Transportation Fact Book*, 16.

and hydrogen fuel cells. As a result, transit agencies are having to transform their operations and maintenance facilities and adopt new, connected, operational technology to accommodate these new vehicles. Doing so creates new vulnerabilities that need to be managed.

Public transportation agencies are also becoming "mobility hubs," where riders can manage their use of public transit as well as MOD services that are often provided by private companies such as shared-use cars, scooters, bikes, taxis, or autonomous vehicles, increasing the number of possible cybersecurity vulnerabilities.



(a) includes Battery-Electric, Hydrogen and Propane Buses

SOURCE: 2023 APTA VEHICLE DATABASE

Figure 9. Percentage of Buses by Fuel Type over Time[26]

This changing transportation environment is forcing transit agencies to modify their business strategies as well as their offerings. Are they bus, train, and subway organizations, or mobility providers? If they are mobility providers, how do they compete or partner with massive Silicon Valley companies such as Alphabet or Uber, or with nimble start-ups such as Via, Swiftly, or Lyft?

COVID exacerbated the need for transit agencies to adapt and change; with office workers commuting less, or not at all, many transit agencies have had to completely rethink their service delivery. Currently, transit ridership demand has moved to the middle of the week and weekends to accommodate changing work schedules. Travel patterns will continue to evolve as corporate work-from-home policies adapt. To succeed, transit agencies need not "do it all." They will continue to outsource aspects of operations where outsourcing is viewed as a more efficient means to deliver services. Transit agencies need to focus on what they do well, contract out what they do not, and leverage technology and data wherever possible. Meeting ridership demand requires adopting new technologies and services that transit operators are beginning to understand, but

[26] Dickens, *2023 Public Transportation Fact Book*, 15.

have not fully integrated into their security operations. This technological evolution comes with an increase in cybersecurity vulnerability.

3.1 Trends in Transit

Public transit agencies contract out many aspects of their operations and systems with increasing regularity. Most agencies have historically contracted with a small number of companies that have dominated the market with proprietary hardware and software. One Chief Innovation Officer the authors interviewed shared that their organization,

> … had one bus OEM (Original Equipment Manufacturer), a CAD-AVL (Computer Aided Dispatch-Automatic Vehicle Locator) provider, two fare providers, and several small specialty vendors that provided most of our software and hardware. Moreover, we were locked into an on-premises network environment that was becoming increasingly difficult to maintain. After a cybersecurity breach, we were forced to modernize our network, move services to the cloud where possible, and look to implement a more interoperable infrastructure.[27]

In a world of on-demand travel, TNCs, artificial intelligence, and multimodal trip planners, incumbent vendors are under direct threat from start-ups and new entrants that are adept at integrating with application program interfaces (APIs). The age of the one-stop shop for an agency's technology needs is waning. Many incumbent vendors will not survive unless they change and adapt to the needs of the transit operator, but neither will the average public transit agency if it does not adapt to the changing nature of the market.

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

Companies such as Uber, Lyft, and Waymo have been able to lure riders away from traditional fixed-route and on-demand services, creating direct competition with public transit agencies for ridership. To address this, many public transit agencies have partnered with these same companies to provide new or expanded service offerings. Mobility-on-Demand (MOD) providers are also competing with public transit agencies for the same riders. Historically, transit agencies have provided defined first- and last-mile services, paratransit supplements, or micro-transit services. APTA's *2022 Fare Database* recorded 117 U.S. transit agencies with mobility pilots, either with

[27] Author interview, August 5, 2024.

Uber, Lyft, other private operators, or in-house operators.[28] Some agencies are now evolving into mobility hubs for an entire region.

Many private companies, such as Via and The Routing Company, serve as vendors for MOD services to transit agencies, while others, such as Uber and Lyft, are partnering with transit agencies and continuing their own private operations separate from transit agencies. Many public transit agencies offer their own version of MOD services. Each has its own platform for data management, privacy, and risk. As transit agencies have struggled with this new paradigm, so too have private vendors. Some have failed, such as Proterra, Nova Bus, and EasyMile. Others have consolidated or have been purchased: Intel bought Moovit; Via bought Remix; Swiftly bought HopThru; and Trapeze entered into strategic partnerships with Masabi and Vontas. The key takeaway from this changing mobility landscape is that it will continue to be unstable and that the transit experience will be based on new forms of connectivity, which creates new threat vectors.

3.2 Risk in Transit

As noted above, failing to modernize could result in a public transit agency becoming irrelevant, but modernizing carries with it the risk of exposing riders, and their staff, to a different, growing array of threats. Unfortunately, those transit agencies that have learned to adopt new technologies to improve efficiency in operations have not necessarily adopted technology to minimize vulnerability to cybersecurity threats at the same rate.[29]

Transit Agencies Struggle to Stay Current with Cybersecurity Challenges

In 2019, MetroLINK suffered a cybersecurity breach. Two years later, MetroLINK obtained a grant from the FTA's Research Demonstration Grant Program that provided them with funding to conduct a cybersecurity assessment and to develop the Cybersecurity Assessment Tool for Transit (CATT),[30] a free publicly available tool that can be accessed from the FTA. CATT is a NIST Cyber Resilience Review (CRR)-based cybersecurity self-assessment tool for transit agencies. Since developing CATT, Mr. Nelson and his team have spent the past several years barnstorming meetings across the country and evangelizing about the risks presented by cybersecurity criminals and actions that can be taken to minimize the impact of a breach. Mr. Nelson says he has made this investment because,

[28] Matthew Dickens and David Kahana, *Public Transportation Fare Database* (APTA, 2022), 226–231, https://www.apta.com/research-technical-resources/transit-statistics/fare-database/.

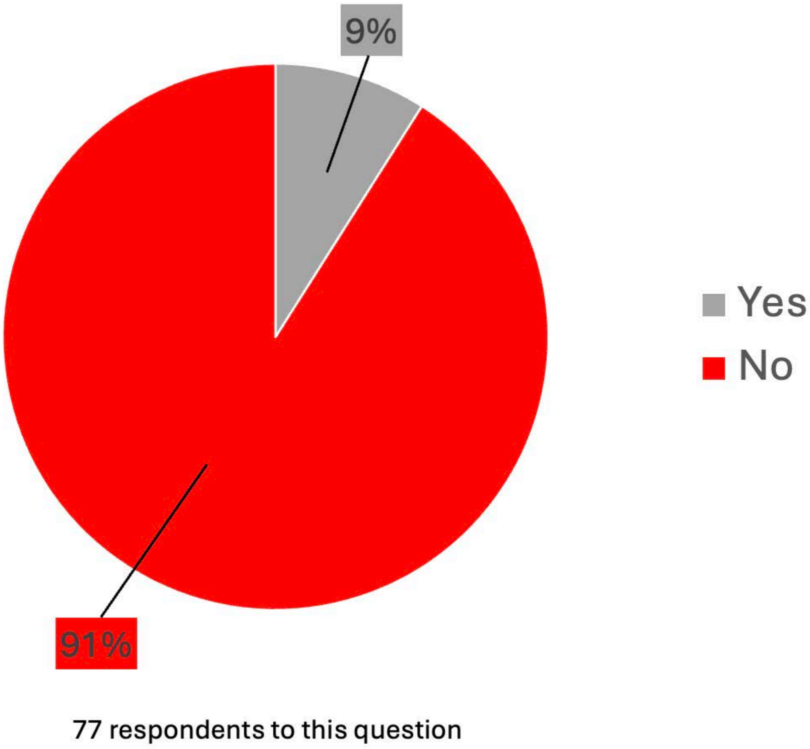
[29] "How Cyber Attacks Are Impacting Transportation Systems," American Journal of Transportation (AJOT), August 22, 2024, https://www.ajot.com/news/how-cyber-attacks-are-impacting-transportation-systems.

[30] "Cybersecurity Assessment Tool for Transit (CATT)," FTA, updated June 21, 2023, accessed August 29, 2024, https://www.transit.dot.gov/research-innovation/cybersecurity-assessment-tool-transit-catt.

> After experiencing our own breach, it became imminently clear how serious the cybersecurity threat is and how ill-prepared we were to respond. We are a relatively well resourced and technologically capable small transit agency, yet we had not invested adequately in reducing the likelihood of a cybersecurity attack or in preparing to respond. After the MTI study came out, I realized that we were not alone and that something had to be done to help small, rural and mid-size agencies understand the risk and put in place the tools to minimize the chance of a breach and mitigate the damage when it inevitably occurs.[31]

As outlined in the findings section, the 2024 survey data continues to reveal poor levels of adoption of cybersecurity measures, especially among rural, small-, and mid-sized transit agencies. Even more concerning, the data shows that agencies continue to under-appreciate or not understand the nature of cyber threats. Furthermore, agencies do not recognize how vulnerable their organizations really are. Most of the agencies that responded to the survey claimed they had not had a cybersecurity incident in the past year. Of the 78 agencies that responded to this question, only seven (9%) answered that they had experienced a cybersecurity incident where more than 1,000 records were breached, over $10K in losses was incurred, or an operating system was down for more than one hour in the last year.

[31] Author interview, May 7, 2024.



77 respondents to this question

Figure 10. Percent of Agencies Reporting an Incident in the Past Year

There is a fair amount of reporting that demonstrates that organizations are being attacked daily. In 2023, Dell Technologies surveyed over 1,500 IT professionals from public and private organizations with more than 250 employees from various industries and learned that in 2023, 90% had suffered a disruptive incident defined as downtime or data loss. More specifically, 52% suffered a cybersecurity attack or other cybersecurity incident.[34]

[34] "Global Data Protection Index Survey – Special Edition 2024," Dell Technologies, October 2023, 8, accessed August 29, 2024, https://www.dell.com/en-us/lp/dt/data-protection-gdpi.

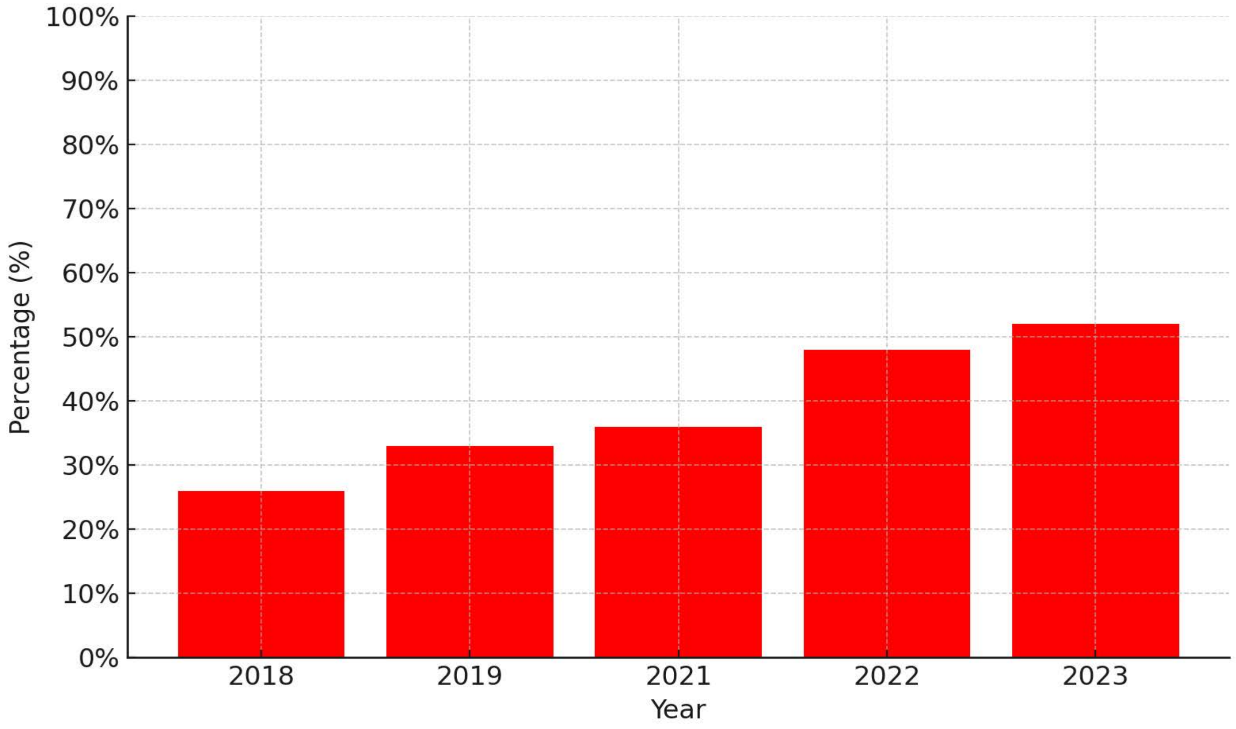


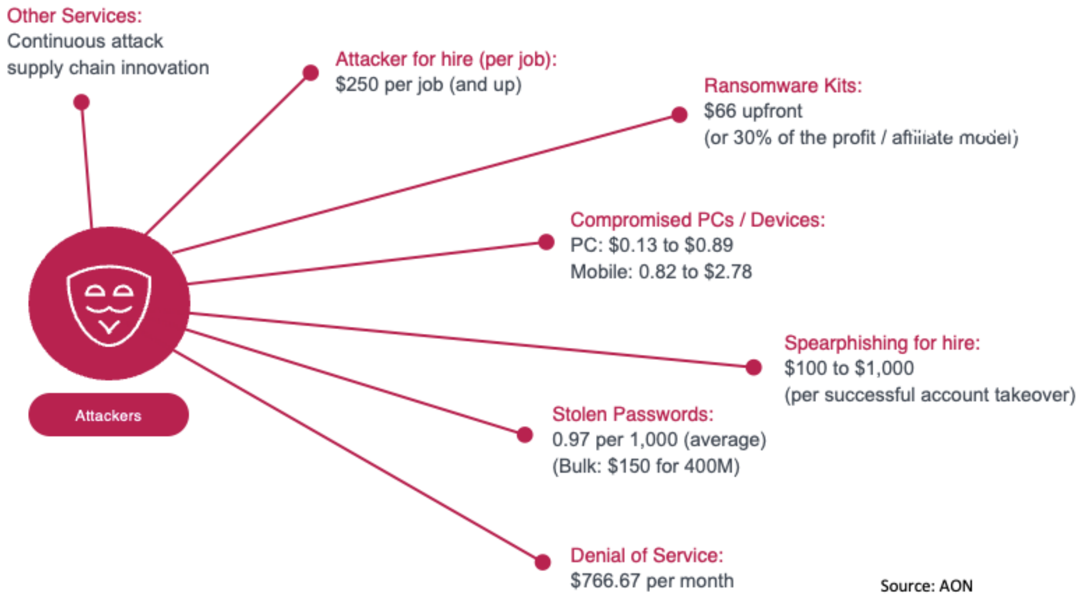
Figure 11. Percentage of Organizations Experiencing a Cyberattack from 2018–2023[35]

3.3 Threats to Transit

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

Figure 12, presented by AON—a global services firm focusing on risk mitigation—at a transit conference in 2023, shows how criminal cybersecurity services have become a commodity: a cybersecurity criminal can purchase a ransomware kit for $66 or 30% of the profit, a successful spear phishing attack for less than $1,000, and 400 million stolen passwords for $150. In combination with the advent of artificial intelligence and bots, it is no wonder that successful cybersecurity attacks are a daily occurrence.

[35] “Global Data Protection Index Survey,” 7.



Source: AON

Figure 12. Cyber-attack as a Service

Data Breaches

Data breaches have become a big part of the general consciousness as more and larger breaches of prominent organizations are reported each year. Data breach threats constantly change as new techniques are developed and technology evolves. Verizon's 2024 Data Breach Investigations Report found that of the "30,458 real world security incidents [reported], 10,626 were confirmed data breaches and that credential-based attacks had been involved in the most data breaches, followed by phishing and vulnerability exploitation, most of which were attributed to an employee opening or clicking on a link in a fraudulent email or website."[36] This type of breach is most often reported because it affects customers and/or employees and the possible loss of their personally identifiable information (PII). The primary impact on companies suffering a data breach is the cost associated with (1) technical remediation of the breach, (2) notification to the victims, and (3) provision of defense against numerous lawsuits (e.g., from customers, shareholders, and state attorneys general). In a 2024 report, IBM and the Ponemon Institute estimated the average cost of a breach in the United States at $4.88 million.[37]

Victim notification requirements are driven by state law, which can vary significantly from one jurisdiction to the next. This effectively amounts to an additional (and complex) set of compliance requirements in addition to Federal reporting requirements.

[36] C. David Hylender, Philippe Langlois, Alex Pinto, and Suzanne Widup, *2024 Data Breach Investigations Report* (Verizon Business, May 1, 2024), 5, verizon.com/dbir.
[37] IBM Security, *Cost of a Data Breach Report 2024* (IBM, July 30, 2024), 9, https://www.ibm.com/reports/data-breach.

There have been several recent high-profile incidents causing regulators to take a more active role to investigate data breaches. A 2024 Baker Hostetler Report found that 28% of breaches requiring notification resulted in a regulatory investigation.[38]

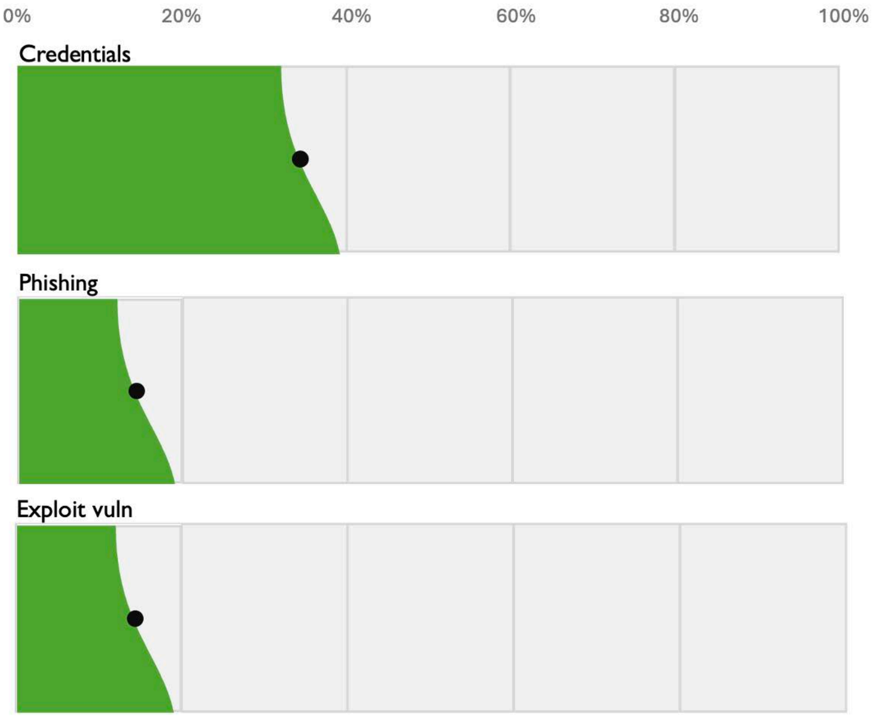


Figure 13. Entrance Points for Data Breaches in 2023[39]

Credential-Based Attacks

Credential-based attacks have become the most common cause of data breaches. This attack type encompasses incidents ranging from third-party data leaks of credentials to social engineering attacks. Credential theft was the initial access vector in 38% of data breaches,[40] making it a significant weak point across the cybersecurity sector.

Credential theft can be particularly difficult to detect because stolen credentials allow an attacker to impersonate an authorized user. Network and access monitoring paired with an effective incident response can mitigate the effects of credential theft, but the best way to protect against this type of attack is to prevent it from happening.[41]

[38] *Data Security Incident Response Report* (BakerHostetler, April 23, 2024) 9, https://admin.bakerlaw.com/wp-content/uploads/2024/04/2024-DSIR-Report-Web.pdf.
[39] Hylender, Langlois, Pinto, and Widup, *2024 Data Breach Investigations Report*.
[40] Hylender, Langlois, Pinto, and Widup, *2024 Data Breach Investigations Report*, 7.
[41] "What is Credential Theft?" SentinelOne, accessed August 29, 2024, https://www.sentinelone.com/cybersecurity-101/what-is-credential-theft/.

Multi-factor authentication and rigorous password protection policies and procedures are key tools to prevent successful credential-based attacks. Multi-factor authentication requires a user to present at least two ways of identifying themselves, usually via a password and a device-based prompt, such as a text, email code, or phone call. Multi-factor authentication has been considered an industry best practice for years and has been specifically recommended by NIST since 2006. However, the authors were under the incorrect assumption that MFA and password protection policies had been widely adopted throughout the transit industry to such an extent that they were not included as survey questions. Based on interviews during the study, it became clear that many agencies still lack formal MFA and password policies or, if they have them, they often fail to enforce them. This gap underscores a critical need for increased awareness and implementation of basic cybersecurity measures.

It is crucial to have a strong password policy that requires complex passwords and a good security training program which reminds users not to reuse passwords or share them with others and helps them identify suspicious credential requests. It is also important to use password managers with breach monitoring systems. These password managers make it easier for users to use novel, complex passwords and allow organizations to monitor data breaches and criminal websites for stolen passwords.[42]

One small agency that was interviewed stated that "given the wide variety of ways a criminal can gain access to stolen credentials, requiring more than one method of identity verification to login into systems and networks is essential."[43] Compare this with the small Community Action Agency (CAA) that has been struggling to keep in place the basic credentialling programs they adopted after a breach.

A Successful Credential-Based Attack Severely Impacted a Small Agency's Ability to Serve Their Customers

> After a credential-based attack, a small CAA began to see communication from its transportation services shut-down. The IT staff immediately shut down the IT systems throughout the rest of the entire CAA, which provides a number of other services in addition to transit to the needy in their community. 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

[42] "Require Strong Passwords," Cybersecurity & Infrastructure Security Agency (CISA), accessed August 29, 2024, https://www.cisa.gov/secure-our-world/require-strong-passwords#:~:text=Require%20strong%2C%20unique%20passwords.,of%205%20%E2%80%937%20random%20words.

[43] Author Interview, August 7, 2024.

> eventually restart other CAA systems. The CAA worked with its employees to establish a cyber-awareness culture, but it is still in need of a comprehensive cybersecurity assessment. The IT staff updated policies regarding passwords, multi-factor authentication, data access, and cybersecurity educational updates, but there is still much more to be done. Competing priorities and limited resources are stalling efforts by leadership to implement the updated policies and take further action. Moreover, the transportation lead observed that "my staff can't wait until we return to normal operations and do not have to do this stuff anymore."[45]

Social Engineering Attacks

Social engineering attacks can include pretexting, phishing, and extortion and are among the most common ways a threat actor can steal credentials for a credential-based attack. Social engineering attacks can also directly steal data and money without ever stealing credentials or directly accessing a system. The three main types—pretexting, phishing, and extortion—make up the majority of social engineering attacks.

[45] Author Interview.

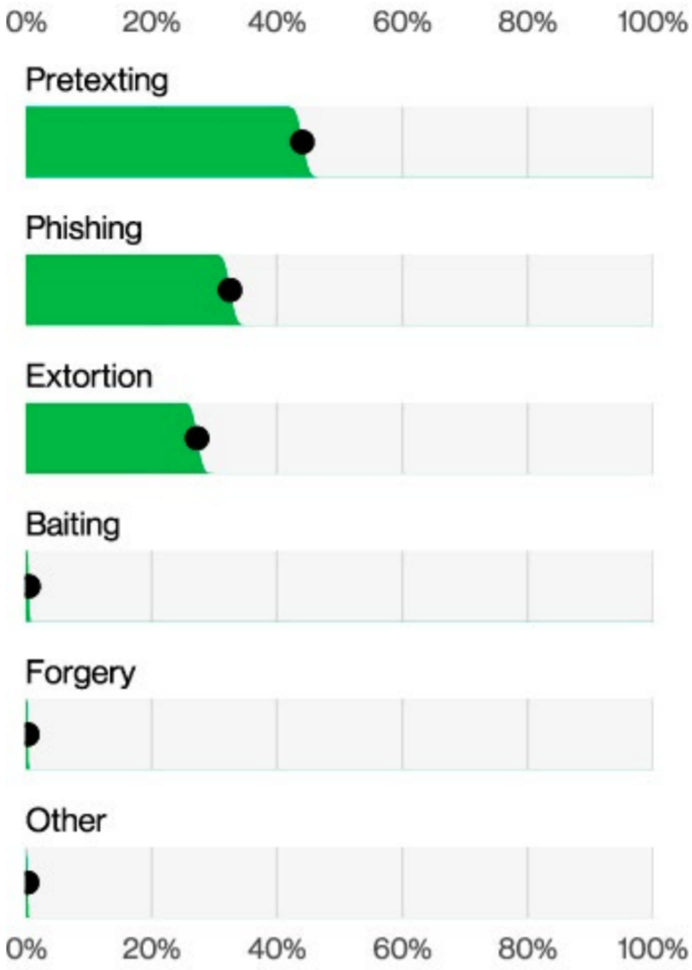


Figure 14. Relative Frequency of Types of Social Engineering Attacks[46]

- **Pretexting** is a type of social engineering attack; one that is particularly dangerous to organizations such as transit agencies. This attack is like phishing in that its aim is to trick users into revealing information they would not otherwise disclose. The main difference between phishing and pretexting, however, is the level of effort and specificity. A phishing attack may send out hundreds of thousands, if not millions, of emails with links to malware or requests for credentials, hoping that even a small number of people will fall for the scam. A pretexting attack uses specific information about an organization to impersonate a trusted individual like an executive or a vendor. They may then utilize this trust to acquire a specific piece of information, document, or credential.

- **Phishing** is the fraudulent attempt to obtain sensitive information such as usernames, passwords, and credit card details, by disguising oneself as a trustworthy entity in an electronic communication. In the most common vector for phishing attacks, the malicious actor induces the recipient, typically through email, to click on a link that sends the

[46] Hylender, Langlois, Pinto, and Widup, *2024 Data Breach Investigations Report*, 37.

recipient to a website that either directly drops malicious code on the recipient's computer or tricks the recipient into revealing account credentials (username and password), enabling the attacker to then impersonate the recipient and gain access to that account.[47]

- **Extortion** involves cybercriminals demanding payment or other concessions from a victim by threatening to expose sensitive data, disrupt operations, or carry out other malicious actions. This often occurs through tactics such as ransomware attacks, where data is encrypted and held hostage, or "double extortion," where attackers threaten to release stolen data publicly if demands are not met. The goal of extortion is to coerce victims into complying with the attackers' demands, typically for financial gain.

Business Email Compromise (BEC) is a more targeted and sophisticated form of social engineering attack, in which the malicious actor impersonates a CEO or other high-level official within a company, usually with the intent of tricking the recipient into transferring money to a bank account controlled by the malicious actor. This type of attack uses elements of a pretexting attack to gain the trust of a system user. In 2023, the FBI reported that thieves used BEC frauds to collect more than $50 billion between 2013 and 2022; $2.9 billion was stolen across 21,489 incidents in 2023.[48]

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

PCI Security

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

[47] "Avoiding Social Engineering and Phishing Attacks," CISA, February 1, 2021, accessed August 29, 2024, https://www.cisa.gov/news-events/news/avoiding-social-engineering-and-phishing-attacks.

[48] *Federal Bureau of Investigation Internet Crime Report 2023* (FBI, March 6, 2024), 11, https://www.ic3.gov/AnnualReport/Reports/2023_IC3Report.pdf.

PCI Security

The PCI Security Standards Council touches the lives of hundreds of millions of people worldwide. As a global organization, it maintains, evolves, and promotes PCI standards for the safety of cardholder data worldwide.

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

The Council has two priorities:

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

In their goal to serve as a global forum for data protection, the Council employs four key pillars to ensure the success of their strategic framework:

- Increasing industry participation and knowledge
- Evolving security standards and validation programs
- Securing emerging payment channels
- Increasing standards alignment and consistency[49]

In 2021, in response to the COVID-19 pandemic and the international increase of remote work, the PCI SSC released a "Work from Home Security Awareness Training."[51] By working remotely, many employees connect to the internet through public networks or wireless access points, which increases the security risk for company and consumer data. Practices of note in the video training module include utilizing Virtual Private Network (VPN) connections while working at home, changing default passwords on home networks, and ensuring that employees do not install or use

[49] "PCI Security," PCI Security Standards Council, accessed July 9, 2024, https://east.pcisecuritystandards.org/pci_security/.

[51] "PCI SSC Work from Home: Security Awareness," PCI Security Standards Council, accessed August 29, 2024, https://blog.pcisecuritystandards.org/new-training-work-from-home-security-awareness.

unapproved hardware or software. The training is set up as a self-guided, easily accessible module for employees with varying levels of technical experience.

Figure 15 shows responses to the 2024 survey question about payment processing. Of the public transit agencies surveyed, two-thirds reported not managing customer payment information. This focuses data security less on the agency and more on the vendor, and the vendors who process payments are subject to strict security standards under PCI DSS. Agencies that outsource these functions must clearly require PCI DSS and an appropriate level of cybersecurity protection in their contract documents to protect themselves.

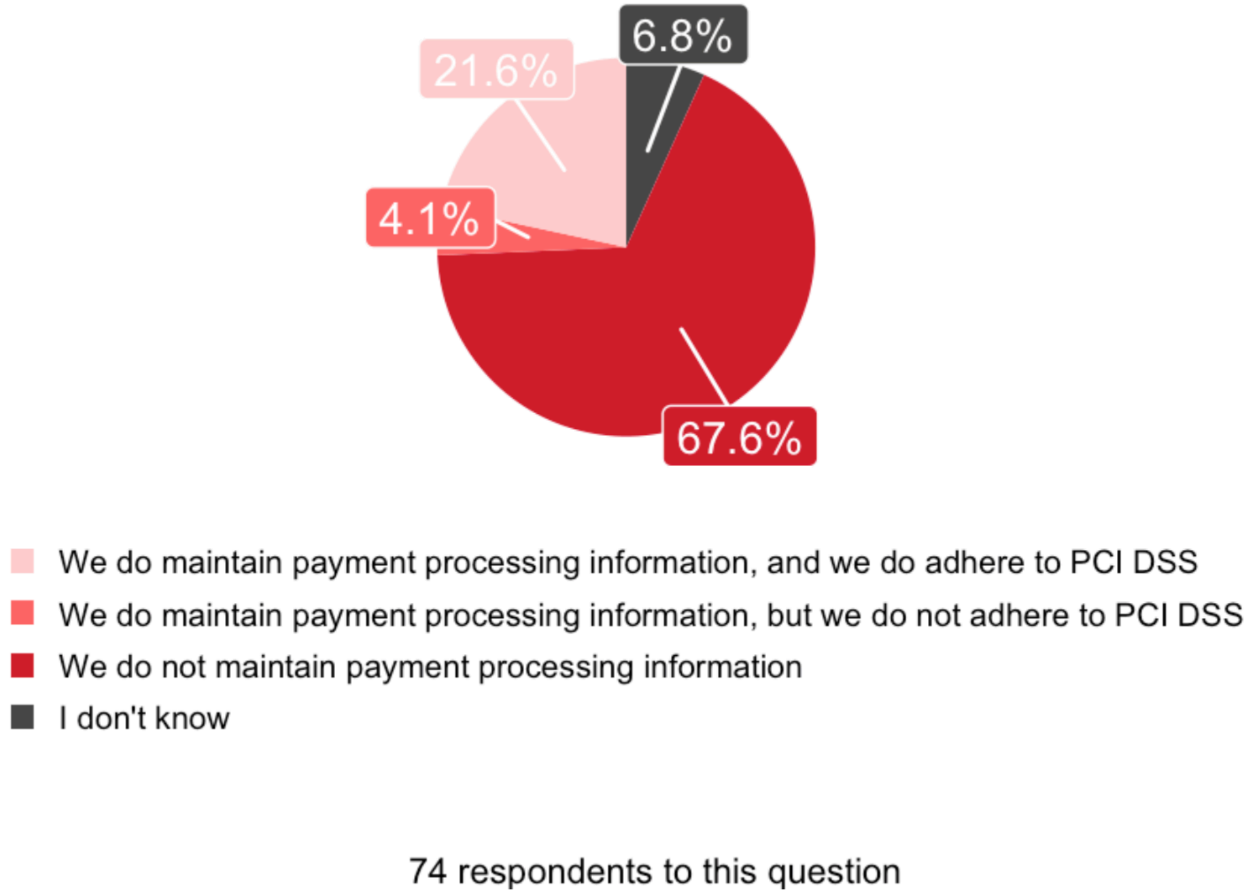


Figure 15. Do you process and/or store customer payment information directly?

Although most transit agencies outsource their payment activities, all transit agencies have little choice but to retain sensitive data on their own employees, which often includes social security numbers, dates of birth, and other critical identifying information. This type of data, while usually found in smaller volumes than payment data, is often valuable to criminals, as there is a robust black market for the sensitive information found in employee records. At many transit agencies, the tools used to manage this data are rudimentary. Sharing is conducted using spreadsheets, email, and other unsecure channels.

3.4 Compromise of Operational Networks

While transit agencies are justified in focusing on the loss of customer and employee data, the compromise of operational data, such as running industrial control systems, traffic signals, and emergency communications networks, brings with it the potential for far more destructive consequences. Experts believe that there is not enough focus on operational technology and business interruption concerns.[52]

Unlike other industries, where the potential consequences of poor cybersecurity are primarily finance driven, an attack on public transit has the potential to be deadly. Vulnerable supervisory control and data acquisition (SCADA) systems could be hijacked by terrorists or cyber-criminals in order to cause derailments or collisions.

Best practice operational security would dictate isolating these networks from the internet, only allowing access from within a transit agency's physical facilities, software updates, and patch management. However, a poor understanding of security practices and the compelling desire for efficiency that comes with remote access and operation frequently override what should be an imperative to protect these critical systems. At the 2024 APTATech conference, Tariq Habib, the Chief Information Security Officer for the New York Metropolitan Transportation Agency, stated that he "had not seen a wholistic or complete cybersecurity in place in any agency to protect and respond to cybersecurity threats."[53] This quote is from the individual overseeing cybersecurity operations for one the largest transit agencies in the world and a recognized industry leader.

3.5 Ransomware

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

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

The demands vary, and almost always include requests for ransom payments and threats to release data. When deadlines for payment are missed, there are more threats, higher ransom demands,

[52] Charles Snyder and Rex Johnson, "Critical Infrastructure and the Rising Threats to Operational Technology," CAI, 2022, accessed August 30, 2024, https://www.cai.io/resources/thought-leadership/critical-infrastructure-and-the-rising-threats-to-operational-technology#fn:4.

[53] "CIO Roundtable: The Convergence of OT & IT," Roundtable, 2024 APTAtech Conference, Philadelphia, PA, August 3, 2024.

and further threats to destroy files. If the business attacked does not pay, the criminals may withhold the decryption keys, making the stolen data permanently unretrievable.

Ransomware Attack on the City of Columbus Results in Major Operational Impacts

> In July 2024, the government of the city of Columbus, Ohio reported a ransomware attack orchestrated by the international cybercrime group Rhysidia. The attackers were able to steal 6.5 terabytes of city data, including employee information, passwords, surveillance video, and access to city systems. The ransomware group demanded a ransom of close to $2 million, threatening to release the city's data if their demands were not met.[54]
>
> The attackers also encrypted systems, preventing IT staff and other city employees from accessing critical data and information. To secure a ransom, the attackers released some of the data on the dark web and conducted several auctions to sell the data online. Cybersecurity experts call this technique "double extortion," where a cybercriminal attempts to extract a ransom both by preventing access to important systems and by threatening to leak captured data.[55]
>
> Columbus officials, working with the FBI and other federal authorities, did not pay the ransom and instead attempted to contain the attack by severing the city's computer system's access to the internet.[56] This course of action did not prevent the attackers from exfiltrating terabytes worth of data, and it resulted in many government systems experiencing significant outages. Government email was down for over a week, website issues persisted, and the computer-aided dispatch system used for first responders was impacted. There have been reports of city employees' bank accounts being hacked, including at least twelve police officers' accounts.[57]

For transit agencies, ransomware presents a large risk. If malicious actors can lock up critical data, the result could be suspension of all operational activity. If that happens, organizations are left to restore access on their own, rely on data archives (if they have them), or use other resources to restore systems. While this might be feasible for some transit agencies, it is certainly not an option

[54] Bill Bush, "Hackers Release Reams of Stolen Columbus Data on Dark Web," *The Columbus* Dispatch, updated August 8, 2024, https://www.dispatch.com/story/news/local/2024/08/08/city-columbus-data-public-dark-web-ransomware-hack-cyber-ohio-cybersecurity-stolen/74718671007/.

[55] Mark Feuerborn, "Columbus Ransomware Attack: Rhysida Starts Data Leak before Changing Course," NBC4i, August 14, 2024, https://www.nbc4i.com/news/local-news/columbus/columbus-ransomware-attack-rhysida-announces-public-leak-before-changing-course/.

[56] "Columbus Thwarted Ransomware Encryption if its IT Infrastructure," The City of Columbus, July 29, 2024, accessed August 29, 2024, https://www.columbus.gov/News-articles/City-of-Columbus-Thwarted-Ransomware-Encryption-of-its-IT-Infrastructure.

[57] Feuerborn, "Columbus Ransomware Attack."

for all, especially those that have not planned for such a scenario. This underscores the importance of conducting frequent system backups, rigorously testing recovery processes, and implementing other best practices such as network segmentation to limit the spread of attacks and mitigate potential damage. Proactive planning and preparedness are essential to safeguarding transit operations against ransomware threats.

The strategy promoted by law enforcement has long been to discourage paying ransom demands. In fact, in 2024, the White House convened the International Counter Ransomware Initiative (CRI) for its fourth meeting in Washington, D.C. to decide on how best to combat ransomware.[62] Following that meeting, Ann Neuberger, U.S. Deputy National Security Advisor for Cyber and Emerging Technologies, wrote in a *Financial Times* opinion piece that "insurance policies – especially those covering ransomware payment reimbursements – are fueling the very same criminal ecosystems they seek to mitigate and is a troubling practice that must end."[63]

Reports from the FBI's Internet Crime Complaint Center state that after a slight decrease in 2022, ransomware incidents saw an increase in 2023 of roughly 18%, for a total of 2,825 reported attacks. Reported losses increased by 74%, from $34.3 million to $59.6 million.[64] According to the FBI's recent infiltration of the Hive ransomware group infrastructure, only about 20% of Hive's victims reported to law enforcement, which affects FBI insight. Emerging trends in ransomware activity were observed by the FBI, such as repeat attacks on the same victim, as well as new data-destruction strategies to push victims to negotiate.[65]

In 2023, ransomware payments exceeded $1 billion, the highest amount ever recorded. The most recent NetDiligence Cyber Claims study demonstrated that this number indicates that ransomware is "one of the main drivers of insurance claims loss for small and medium enterprises including public transportation."[66]

[62] The White House, "FACT SHEET: Biden-Harris Administration Convenes Fourth Global Gathering to Counter Ransomware," fact sheet, October 2, 2024, https://www.whitehouse.gov/briefing-room/statements-releases/2024/10/02/fact-sheet-biden-%E2%81%A0harris-administration-convenes-fourth-global-gathering-to-counter-ransomware/.

[63] Ann Neuberger, "The Ransomware Battle is Shifting – So Should Our Response," *Financial Times*, October 3, 2024, accessed October 10, 2024.

[64] *Internet Crime Report 2023*, 11.

[65] "Director Christopher Wray's Remarks at Press Conference Announcing the Disruption of the Hive Ransomware Group," FBI, January 26, 2023, accessed December 12, 2024, https://www.fbi.gov/news/speeches/director-christopher-wrays-remarks-at-press-conference-announcing-the-disruption-of-the-hive-ransomware-group.

[66] Scott Belcher and Todd Chollet, "Is There a Light at the End of the Tunnel? The Outlook for Cybersecurity Insurance and Transit in 2024," Mineta Transport Institute, April 24, 2024, accessed September 8, 2024 https://transweb.sjsu.edu/press/There-Light-End-Tunnel-Outlook-Cybersecurity-Insurance-and-Transit-2024.

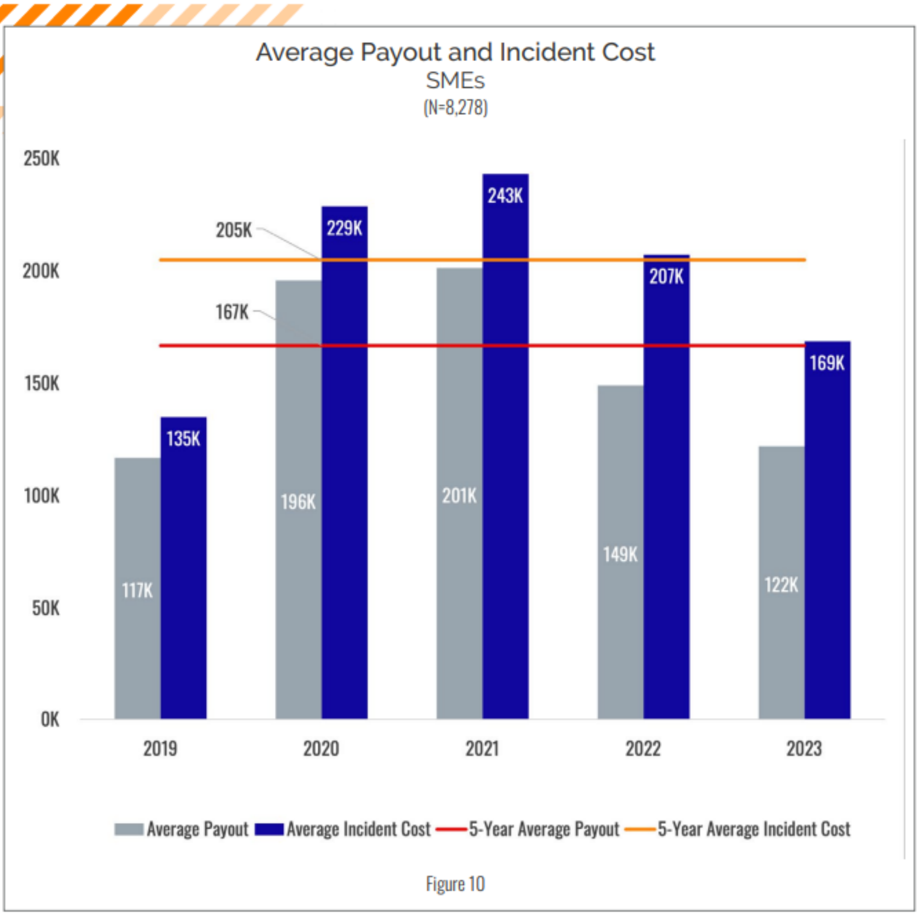


Figure 16. Average Ransomware Payout 2019–2023[67]

[67] *NetDiligence Cyber Claims Study 2024 Report* (Net Diligence, 2024), 9, https://netdiligence.com/wp-content/uploads/2024/09/NetDiligence-Cyber-Claims-Study-2024-Report-1.pdf.

The Decision about Whether to Pay a Ransom is Complicated and Expensive Regardless of What an Organization Chooses to Do

> Regardless of whether a ransom is paid, recovery from an attack can severely impact operations. In June 2024, Oahu Transit Service (OTS) suffered its second cyber incident in three years. In this ransomware attack, the personal data of users of The Handi-Van and The Bus (OTS's primary bus service) was impacted. The attack forced OTS to temporarily shut down bus service, websites, GPS monitoring, phone service, fare card readers, and digital communications with the city and the vendors that manage their payment services to limit the malware spread. It took several weeks to bring many of the systems back online as OTS was forced to disinfect hundreds of computers. The attackers demanded a ransom payment which was not paid.[68]

3.6 Vendor Management

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

Vendors are a common attack vector for malicious actors, as those companies often have close working relationships with their customers, especially in transit which is heavily dependent on third-party vendors. The exploitation of this relationship can be simple or complex. In a simple attack, an attacker may fool an employee to click on a harmful link in an email that appears to be coming from the vendor. In a more complex attack, the attacker could compromise a direct connection between the vendor's network and that of the transit agency. In 2024, Ken Weeks, the CISO in New Hampshire, was quoted about his two-year tenure: "any significant data breach that's occurred for data of New Hampshire residents at the state government level, or significant loss of service due to a cyber incident, has been with a third-party partner that helps us deliver those government services."[70] In its recent report on data breaches, Verizon concluded that supply

[68] Mahealani Richardson, "Rider Data Apparently Compromised in Alleged Ransomware Attack on The Bus and Handi-Van," Hawaii News Now, June 18, 2024, accessed November 21, 2024, https://www.hawaiinewsnow.com/2024/06/19/ots-cyber-breach-allegedly-includes-800000-pieces-data/.

[70] Jule Pattison-Gordon and Noelle Knell, "How Two States Handle Cyber Security Risks from Vendors," Government Technology, October 10, 2024, https://www.govtech.com/security/how-two-states-handle-cybersecurity-risks-from-vendors?utm_campaign=Newsletter%20-%20GT%20-%20GovTech%20Today&utm_medium=email&_hsenc=p2ANqtz--DzlazjWlIKaNNTtQM3PPFAL_EHvV8zGIv978bYkp9Z3K3wZEWJHjYk4hlCFQe8SrnZCcYyWW-3VRWWtaURedMF82eJw&_hsmi=329834740&utm_content=329837483&utm_source=hs_email.

chain attacks are now the preferred method used by threat actors, and 62% of network intrusions originate with a third-party—often someone in the software supply chain.[71]

The survey responses indicated that 47.4% of public transit agencies surveyed said they do not currently have standard clauses related to cybersecurity included in their vendor contracts. An additional 7.7% responded that they did not know whether they included such clauses in their vendor contracts (Figure 17). These numbers are inherently troubling, but they also raise questions as to the sophistication of the standard clauses that transit agencies have inserted in their vendor contracts—and the extent to which the requirements in those clauses are monitored, enforced, or even understood by those who include them in the contracts.

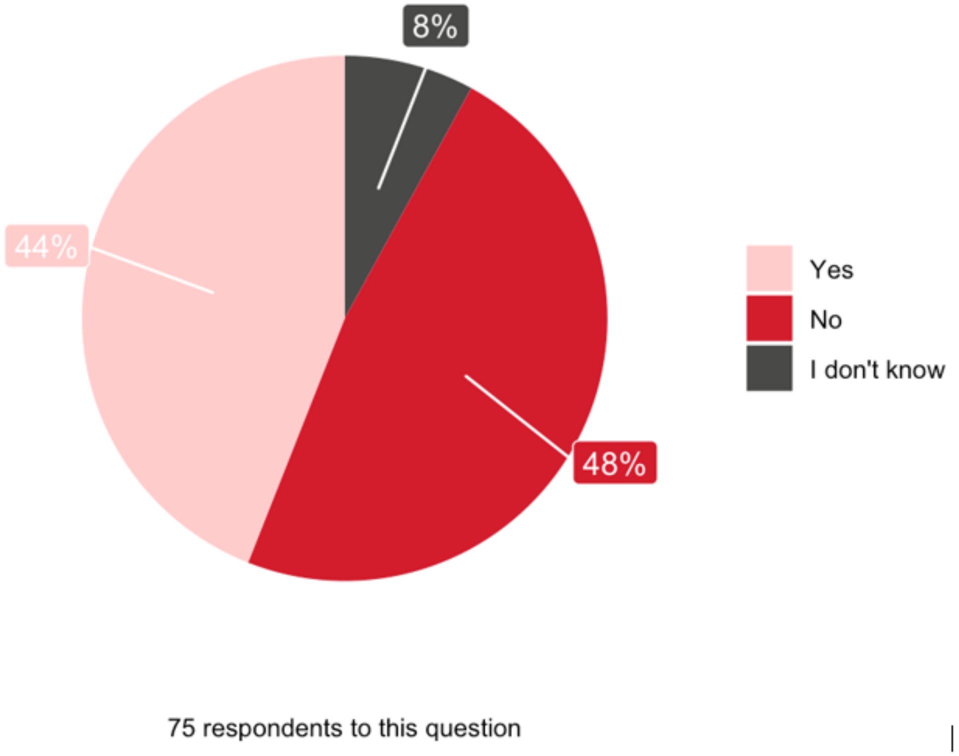


Figure 17. Do you have standard clauses in your vendor contracts related to cybersecurity?

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

Effective cybersecurity management among vendors begins with agencies "passing through" cybersecurity requirements as part of their Request for Proposals (RFPs) and contracts. Several

[71] Timo Burbidge, "Ransomware Threat Rises: Verizon 2022 Data Breach Investigations Report," Verizon, May 24, 2022, https://www.verizon.com/about/news/ransomware-threat-rises-verizon-2022-data-breach-investigations-report.

government organizations have published recommended cybersecurity procurement language for vendor contracts for transit agencies, including the US DOT's Intelligent Transportation Systems Joint Program Office (ITS JPO)[72] and the Joint Office of Energy and Transportation within the US DOT and Department of Energy (DOE),[73] as well as the Edison Electric Institute.[74] These resources universally recommend language that mandates software updates and patches, incident and breach notifications, and vulnerability disclosures. Some also suggest requiring cybersecurity assessments or audits.[75] Audit requirements typically ensure that a third party is engaged periodically to confirm compliance. For some, certain requirements are made clarifying who can provide such audit services, such as firms with U.S. ownership or certain accreditations. Most stipulate how often an external audit must be conducted, as well as the documentation that must be shared with the client.

Software updating and patching requirements involve an initial certification of stability for the software provided, including all updates and patches, as well as requirements for continued support. This continued support can include protection against malware and viruses, warranty guarantees, and formal patch management plans.[76] Incident or breach notification language requires vendors to notify a designated individual or group of any incidents or breaches the vendor experiences. The language also typically outlines the method of notification, what details the notification must provide, the timeframe required, and a clear definition of what constitutes an incident or a breach. Vulnerability disclosure requirements are also universally recommended. These clauses require vendors to disclose all cybersecurity vulnerabilities in their products at the time of delivery as well as continuously notifying the procurer of any new vulnerabilities discovered.[77]

Other language recommendations include specifications regarding what data are tracked and how long they are stored, access control policies, and vendor cybersecurity plans.[78]

[72] Dan Lukasik, Jack Oden, Robert Sanchez, Brian Russell, Kyle Rush, Adam Chandler, "Procurement Language, Cybersecurity, Apps, Intelligent Transportation System, ITS," U.S. Department of Transportation, January 22, 2024, https://rosap.ntl.bts.gov/view/dot/73792.

[73] "Cybersecurity Procurement Language Clauses for RFPs and EVSP Contracts," Joint Office of Energy and Transportation, accessed August 30, 2024, https://driveelectric.gov/cybersecurity-clauses.

[74] *Model Procurement Contract Language Addressing Cybersecurity Supply Chain Risk*, Version 3.0 (Edison Electric Institute, October 2022), https://www.eei.org/-/media/Project/EEI/Documents/Issues-and-Policy/Model--Procurement-Contract.pdf.

[75] Lori Ross O'Neil, Thoams E. Carroll, Entesar M. Abdelhadi, Mark D. Watson, Carol L. Hammer, and Maria B. Psarakis, *Sample Cybersecurity Clauses for EV Charging Infrastructure Procurements* (Joint Office of Energy and Transportation, June 30, 2023), https://www.pnnl.gov/main/publications/external/technical_reports/PNNL-34454.pdf.

[76] O'Neil, Carroll, Abdelhadi, Watson, Hammer, and Psarakis, *Sample Cybersecurity Clauses*.

[77] Lukasik, Oden, Sanchez, Russell, Rush, and Chandler, "Cybersecurity Language for the Procurement of Intelligent Transportation System Equipment."

[78] "Model Procurement Contract Language Addressing Cybersecurity Supply Chain Risk."

The North American Transit Consortium

> A group of roughly 40 leading transit agencies have formed the North American Transit Cybersecurity Consortium, chaired by the Metropolitan Transportation Agency, and have developed an exhaustive Cybersecurity Procurement Requirements Manual for Operational Technology (OT). While the document is still in draft and is largely focused on rail and OT, it presents a wealth of information and establishes a process for "building a centralized cybersecurity strategy that detects, identifies, prevents, circumvents, recovers, and manages the various levels of cybersecurity threats that can jeopardize the railway system."[79] This strategy can be used by most agencies, regardless of whether they operate rail. While many agencies will not be able to deploy all of the technologies suggested, they should be aware that they are industry best practices and utilize the document as a guide where possible.

Transit agencies are struggling to find the correct language to use in their contracts and often use inconsistent and unnecessary language that forces companies to either drop out of a procurement because of the costs of compliance or unnecessarily drive up the cost of compliance. This challenge is addressed in detail in the MTI study *Aligning the Transit Industry and Their Vendors in the face of Increasing Cyber Risk: Recommendations for Identifying and Addressing Cybersecurity Challenges*.[80]

In the face of unrealistic contract demands, a vendor can sometimes work with a transit agency to "right size them." In one example, an ITS vendor was asked to respond to an RFP for a sensor device that they had provided to the agency for many years. The new RFP included cybersecurity language drawn from the Defense Federal Acquisition Supplement that was clearly not applicable. The vendor was able to work with the agency to reach an agreement on reasonable cybersecurity requirements and ultimately won the contract.

Excessive Request for Insurance Requirements in RFP

> One government contractor recounted that his company had recently responded to a Request for Proposal requiring a $50 million cybersecurity policy on a contract that was valued at less than $10 million over three years. He described the contract as a basic technology services contract no different from their other projects of this size, where the amount of cybersecurity coverage required would typically be about $2 million per year. After unsuccessfully questioning the need for that level of coverage, the contractor got bids to provide the level of coverage which averaged

[79] Operational Technology Procurement Requirements, North American Transit Cybersecurity Consortium, January 31, 2024, 5 (accessed March 21, 2025) https://nacitcc.mta.info/NATCA_OT_Procurement_Requirements.pdf

[80] Scott Belcher, Terri Belcher, Kathryn Seekman, Brandon Thomas, and Homayun Yaqub, "Aligning the Transit Industry and Their Vendors in the Face of Increasing Cyber Risk: Recommendations for Identifying and Addressing Cybersecurity Challenges," Mineta Transportation Institute, July 2022, DOI:10.31979/mti.2022.2113.

> $500,000 in annual premiums. Each insurer the company spoke with agreed that this was an unnecessary and unreasonable amount of coverage for the contract. The only way the contractor was able to bid on the contract was to build these costs into their unsuccessful proposal.

Beyond contract clauses establishing cybersecurity requirements, vendor management related to cybersecurity can be valuable for ensuring that necessary measures are in place to reduce exposure and mitigate impacts as incidents occur. Physically reviewing operations and asking questions about access and system credentials can help convey to the vendor the seriousness of cybersecurity. Cybersecurity requirements established through vendor contracts can provide a solid basis on which to manage vendors' cybersecurity practices. This can be an especially valuable tool for those operators that have resource constraints. Mike Kohlman, the Chief Information Officer at the Monterey Salinas Transit Agency, believes that it is also important to actively manage these provisions:

> We had a situation where we identified what appeared to be an intrusion and submitted a ticket to our managed service provider. They weren't concerned because we were operating in a Microsoft environment. When the intrusion appeared to spread, we felt that we had to shut down our server. The vendor remained unconcerned and not very helpful. I escalated it a couple of levels and never got the kind of response I would have expected. It turned out to not be a hack, but I replaced the vendor anyway. We would have been in trouble if it had been real.[81]

3.7 Supply Chain Risk Management

On May 15, 2019, the White House issued Executive Order (EO) 13873, "Securing the Information and Communications Technology and Services Supply Chain," which has had cascading effects for transportation and other sectors.[82] The EO covers broad-based Information Communications Technology (ICT) and supply chain risk, encompassing 5G network gear.

Once a Company from a Hostile Nation Introduces Equipment Posing a Supply Chain Risk, It Can Be Difficult and Expensive to Remove and Replace

> Huawei and the ZTE Corporation, both Chinese multinational information technology and consumer electronics companies, have been accused by the United States and other nations of corporate espionage and intellectual property theft. In 2019, Huawei and ZTE were restricted from engaging in commerce with U.S.

[81] Author interview, August 14, 2024.

[82] Exec. Order No. 13873, 84 Fed. Reg 22689 (May 17, 2019), https://www.federalregister.gov/documents/2019/05/17/2019-10538/securing-the-information-and-communications-technology-and-services-supply-chain.

> companies resulting from allegations that they willfully exported technology of U.S. origin to a hostile nation in violation of U.S. sanctions, having direct implications for transit. In addition to restricting U.S. companies from doing business with Huawei and ZTE, Congress has provided funds to remove them from use in the United States. In fact, on May 2, 2024, the Chair of the Federal Communications Commission (FCC) reported to the Senate that the FCC needed $4.98 billion for the removal, replacement, and disposal of communications equipment and services produced or provided by Huawei Technologies Company and ZTE Corporation, of which Congress had only appropriated $1.9 billion.[83]

In December 2019, President Trump signed into law the National Defense Authorization Act for 2020, which included a provision banning the use of federal funds to purchase "rolling stock" (e.g., cars, vans, buses, rail cars) made by companies "owned or controlled" by countries that the U.S. Trade Representative has identified on its Priority Watch List,[85] including China. This ban took effect December 2021 and immediately impacted BYD, a Chinese electric bus manufacturer with facilities in Lancaster, PA.

In 2021, President Biden signed into law the "Build America, Buy America Act," which was enacted as a part of the Infrastructure Investment and Jobs Act. This statute requires that all iron, steel, manufactured products, and construction materials used in covered infrastructure projects are produced in the United States. This means that any federal funds transit agencies receive for infrastructure projects must be used to buy American-made products and meet the 75% American-made content requirement.[86] These new requirements apply to a variety of grant programs relevant to transit agencies, including Federal Transit Formula Grants, Formula Grants for Rural Areas and Tribal Transit, State of Good Repair Grants, and many others. Of note, BYD USA states that its electric buses now have roughly 75% American content and are Buy America compliant.[87]

These efforts reflect a growing concern over cybersecurity supply chain risk management in the transit sector. Other sectors have been gradually waking up to the realization that the technological equipment they purchase may suffer from pervasive vulnerabilities before it is even connected to their business or operational networks. Whether due to insufficient security in the engineering of the hardware, software, or firmware, compromise of the industrial process by nation-state actors, or active collaboration between the manufacturer and these actors, the reality is that, owing to the

[83] Letter from Jessica Rosenworcel, Chairwoman of the Federal Communications Commission, to the Honorable Maria Cantwell, Chair of the Senate Committee on Commerce, Science, and Transportation, May 2, 2024, https://docs.fcc.gov/public/attachments/DOC-402312A1.pdf.

[85] National Defense Authorization Act for Fiscal Year 2020, , https://www.congress.gov/bill/116th-congress/senate-bill/1790/text.

[86] "Transportation," 49 *Code of Federal Regulations*, Part 661 and "Transportation," 49 *Code of Federal Regulations* Part 663.13.

[87] "Buy America," BYD, accessed October 10, 2024, https://en.byd.com/news/buy-america/#:~:text=All%20our%20bus%20models%20in,American%20vendors%20across%20the%20nation.

highly distributed, global manufacturing process, virtually no supply chain can be guaranteed secure.

NIST 2.0 calls out the importance of supply chain management and has provided additional guidance and tools for managing an organization's relationships with their suppliers, contractors, and partners. The most important of these is the Cybersecurity Supply Chain Risk Management Practices for Systems and Organizations, which the agency describes as:

> a systematic process for managing exposure to cybersecurity risks throughout the supply chain and developing appropriate response strategies, policies, processes, and procedures. The purpose of this publication is to provide guidance to enterprises on how to identify, assess, select, and implement risk management processes and mitigating controls across the enterprise to help manage cybersecurity risks throughout the supply chain. The content in this guidance is the shared responsibility of different disciplines with different SCRM perspectives, authorities, and legal considerations.[88]

3.8 Counterfeit Hardware

The possibility of counterfeit or compromised hardware is a very real risk to any operational agency, including transit. The most public OT-based transit breach occurred in 2017, when, prior to launching its Silicon Valley Berryessa Extension, the Bay Area Rapid Transit (BART) discovered that 86% of their switches had previously been decommissioned in hostile nations. Further research discovered hidden backdoors on the devices, as well as a persistent "ping" where data are sent to a foreign nation hostile to American interests. This OT breach resulted in an international criminal investigation impacting multiple other transit operators doing business with the same contractor and subcontractor that unwittingly purchased counterfeit hardware.[89]

In 2024, the leader of a large group of counterfeit Cisco hardware companies was convicted of trafficking counterfeit and fraudulent Cisco communications equipment. In 2023, the ring of 19 companies sold more than $100 million worth of counterfeit, Chinese-made Cisco hardware. The networking equipment ended up in hospitals, schools, and even sensitive military and other government systems.[90] The threat of counterfeit or compromised hardware remains a very real risk, especially when supply chains are limited and vendors are looking to fill orders or save money.

[88] Jon Boyens, Angela Smith, Nadya Bartol, Kris Winkler, Alex Holbrook, Matthew Fallon, *Cybersecurity Supply Chain Risk Management Practices for Systems and Organizations* (NIST Special Publication, NIST SP 800-161r1, May 2022), https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-161r1.pdf.

[89] Author interview, May 17, 2020.

[90] U.S. Department of Justice, "Leader of Massive Scheme to Traffic in Fraudulent and Counterfeit Cisco Networking Equipment Sentenced to Prison," press release, May 2, 2024, https://www.justice.gov/opa/pr/leader-massive-scheme-traffic-fraudulent-and-counterfeit-cisco-networking-equipment.

3.9 Workforce

One cybersecurity risk for all organizations is the inability to attract and retain the limited cybersecurity talent. This is especially challenging for public sector agencies that cannot match private sector wages. Even large transit agencies that have a CISO and cybersecurity team have had difficulty retaining cybersecurity employees.

Even Large Transit Agencies Face Difficulty Attracting and Retaining Cybersecurity Talent

Taj Jalali was hired into AC Transit in 2019 to build a cybersecurity practice. Within weeks of his hire, AC Transit discovered an ongoing ATO (account takeover) attack that was impacting the entire organization as well as its vendors and partner agencies. Because of the underlying shortcomings of their security email gateway and their lack of organization expertise, they were forced to bring in an outside support to stop the spread and minimize the damage.[91] Since that time, Jalali has been building out a cybersecurity team that consists of internal staff and consultants:

The main challenge we face is attracting and retaining cybersecurity talent. We are in the Bay Area and competition is fierce. Really, we focus on building from within. We use the free resource from CISA, make resources available for training, and have built an internal development structure.[92]

Attracting cybersecurity talent is even more challenging for small- and mid-sized transit agencies. Many do not have specialized IT staff, and hiring cybersecurity staff is not feasible. Transit agencies that are aware of and planning for the risks that cybersecurity poses have addressed it in a variety of different ways: providing existing employees with training, recruiting from other parts of the organization, or augmenting existing staff with contract staff. Contract staff can provide a range of services including managing cybersecurity assessments, documenting policies and procedures, providing training, conducting tabletop exercises, and conducting penetration testing and threat monitoring. Another alternative is to retain the full suite of cybersecurity services, often called "a CISO in a box." It is critical, however, that there be an employee within the organization that is sufficiently knowledgeable about cybersecurity to advise leadership on what is necessary and appropriate for the agency and who can effectively manage the contractor(s).

[91] Dennis Noone, "Transit Agency Faced Growing Problem, Chose Abnormal Solution," Government Technology Industry Insider, March 13, 2023, accessed August 9, 2024, https://insider.govtech.com/california/news/transit-agency-faced-growing-problem-chose-abnormal-solution.

[92] Author interview, August 13, 2024.

Small Agency is Creative in Building Cybersecurity Expertise

Mike Kohlman, from the Monterey Salinas Transit agency, spent most of his career in non-transportation public sector roles and he knew that when he joined MST it would be a challenge to attract cybersecurity talent, so he got creative.

First, I always look at individuals leaving the military. They have solid cybersecurity training as well as a public service orientation and are more easily enticed to join the public sector. Second, I went into the garage where there were smart mechanics who understand operational technology. That is the hardest part to teach, especially when you are talking cybersecurity and transit. Finally, I had to convince my management to invest in cybersecurity whether it meant sending one of the existing IT professionals to an off-site intensive cybersecurity training program or supporting their need to obtain cybersecurity credentials and keep them up to date. I was lucky, I came from a high-risk environment and could speak to the repercussions of not making these types of investments and I have an enlightened executive team.[95]

[95] Author interview, August 13, 2024.

4. Existing Cybersecurity Guidance for Transit

This section provides a broad overview of the guidance, tools, and resources available to the public transit industry. The existing cybersecurity guidance for public transit is spread across several government and industry entities. This overview is not meant to be comprehensive because more resources are becoming available on a regular basis. Rather, it is meant to direct researchers and individual transit agencies towards many of the most meaningful documents or websites that are available today that can guide them in developing their own cybersecurity plans.

While there is abundant guidance to support agencies in developing a cybersecurity plan, there is limited regulatory accountability for agencies that do not avail themselves of these resources, placing their agencies at a heightened risk of a cybersecurity breach.

Because of the ubiquity of the internet, digital, and connected systems, the DHS, U.S. DOT, and other agencies have developed an array of both offensive and defensive tools and tactics to protect from and respond to cyber threats. The bulk of this work is focused on what is deemed to be critical infrastructure.

Critical Infrastructure

> There are 16 critical infrastructure sectors whose assets, systems, and networks, whether physical or virtual, are considered so vital to the United States that their incapacitation or destruction would have a debilitating effect on security, national economic security, or national public health or safety.[97]

The DHS and U.S. DOT are the Transportation Systems Sector (TSS) Co-Sector Specific Agencies that are responsible for public transportation, including mass transit. As such, the DHS and U.S. DOT are not only accountable, but they are also mandated to support the security of America's transit systems, both the physical and digital components. Moreover, as noted above, the risk profile of these systems is increasing as technology evolves. However, to date, the regulatory regime remains behind in establishing the necessary regulation, compliance requirements, oversight, and funding to ensure the nation's transit systems adequately address current and future cybersecurity threats.

In the absence of legislation, the White House has issued a series of Executive Orders to direct federal agencies to enhance their cybersecurity resilience and to establish a comprehensive framework for approaching cybersecurity in the U.S. It is important to recognize that many of the

[97] "Critical Infrastructure Sectors," CISA, accessed August 29, 2024, https://www.dhs.gov/cisa/critical-infrastructure-sectors.

requirements outlined in the Executive Orders flow through to the federal government supply chain as well as to those supporting agencies that receive federal funds.

Key Executive Orders include:

Executive Order 13636, Improving Critical Infrastructure Cybersecurity[99] and Presidential Policy Directive 21 (PPD-21), Critical Infrastructure Security and Resilience[100] tasks the National Institute for Standards and Technology (NIST) to work with the private sector to identify existing voluntary consensus standards and industry best practices and build them into a Cybersecurity Framework. The Directive established that DHS and U.S. DOT share responsibility for the TSS. In sharing this role, the DHS's and U.S. DOT's responsibilities include:

- Collaborating with critical infrastructure owners and operators.
- Coordinating with state, local, tribal, and territorial entities to implement the directive.
- Providing, supporting, or facilitating technical assistance and consultations to identify vulnerabilities and help mitigate incidents in the sector.

Executive Order 13800, Strengthening the Cybersecurity of Federal Networks and Critical Infrastructure clarifies federal agencies accountable for managing cybersecurity risks to their ecosystem and further encourages them to work with all entities to adopt the NIST Cybersecurity Framework.[101]

Executive Order 14028, Improving the Nation's Cybersecurity requires federal agencies to enhance cybersecurity and software supply chain integrity.[102] This Executive Order provides a detailed list of actions that federal agencies should take related to cybersecurity information sharing, reporting, procurement, detection, and response. It also provides direction that these requirements should flow down to government contractors doing business with the federal government.

The White House has been very active in other ways to promote cybersecurity resilience and response activities that are beyond the scope of the report. A good means of understanding the breadth of activities is provided in the Administration's *National Cybersecurity Implementation Plan*, released in 2024.

[99] Exec. Order No. 13636, 78 Fed. Reg. 11737 (February 19, 2013).
[100] Presidential Policy Directive (PPD) 21 (February 13, 2013), https://obamawhitehouse.archives.gov/the-press-office/2013/02/12/presidential-policy-directive-critical-infrastructure-security-and-resil.
[101] Exec. Order No. 13800, 82 Fed. Reg. 22391 (May 16, 2017).
[102] Exec. Order No. 14028, 86 Fed. Reg. 26633 (May 17, 2021).

4.1 The National Institute of Standards and Technology (NIST)

The foundation for much of the U.S.'s cybersecurity efforts, including those by the DHS and the U.S. DOT, is the NIST Cybersecurity Framework (NIST CSF). NIST is a non-regulatory agency that has no authority to dictate the use of any standard. However, when there is a matter of public good that depends on establishing a standard, NIST convenes relevant public and private stakeholders to develop the standard.

Cybersecurity Framework Core Functions

GOVERN, IDENTIFY, PROTECT, DETECT, RESPOND, RECOVER

- **GOVERN (GV)** – The organization's cybersecurity risk management strategy, expectations, and policy are established, communicated, and monitored. The GOVERN Function provides outcomes to inform what an organization may do to achieve and prioritize the outcomes of the other five Functions in the context of its mission and stakeholder expectations. Governance activities are critical for incorporating cybersecurity into an organization's broader enterprise risk management (ERM) strategy. GOVERN addresses an understanding of organizational context; the establishment of cybersecurity strategy and cybersecurity supply chain risk management; roles, responsibilities, and authorities; policy; and the oversight of cybersecurity strategy.

- **IDENTIFY (ID)** – The organization's current cybersecurity risks are understood. Understanding the organization's assets (e.g., data, hardware, software, systems, facilities, services, people), suppliers, and related cybersecurity risks enables an organization to prioritize its efforts consistent with its risk management strategy and the mission needs identified under GOVERN. This Function also includes the identification of improvement opportunities for the organization's policies, plans, processes, procedures, and practices that support cybersecurity risk management to inform efforts under all six Functions.

- **PROTECT (PR)** – Safeguards to manage the organization's cybersecurity risks are used. Once assets and risks are identified and prioritized, PROTECT supports the ability to secure those assets to prevent or lower the likelihood and impact of adverse cybersecurity events, as well as to increase the likelihood and impact of taking advantage of opportunities. Outcomes covered by this Function include identity management, authentication, and access control; awareness and training; data security; platform security (i.e., securing the hardware, software, and services of physical and virtual platforms); and the resilience of technology infrastructure.

- **DETECT (DE)** – Possible cybersecurity attacks and compromises are found and analyzed. DETECT enables the timely discovery and analysis of anomalies, indicators of compromise, and other potentially adverse events that may indicate that cybersecurity attacks and incidents are occurring. This Function supports successful incident response and recovery activities.

- **RESPOND (RS)** – Actions regarding a detected cybersecurity incident are taken. RESPOND supports the ability to contain the effects of cybersecurity incidents. Outcomes within this Function cover incident management, analysis, mitigation, reporting, and communication.

- **RECOVER (RC)** — Assets and operations affected by a cybersecurity incident are restored. RECOVER supports the timely restoration of normal operations to reduce the effects of cybersecurity incidents and enable appropriate communication during recovery efforts improvement opportunities for the organization's policies, plans, processes, procedures, and practices that support cybersecurity risk management to inform efforts under all six functions.[105]

NIST CSF 2.0 also includes organizational template profiles, community profiles generalized for industries, and a variety of follow-on resources designed to help the revised framework fulfill its mission to a wider range of organizations. Transit agencies will find value in the small business quick start guide,[107] designed to help small to medium sized organizations with little to no cybersecurity policies in place; implementation examples, which demonstrate ways the new standards can be met; and the Quick-Start Guide for Cybersecurity Supply Chain Risk Management,[108] which helps agencies apply the CSF standards to their complex supply chains.

4.2 U.S. Department of Homeland Security

In 2015, the DHS built upon the NIST Framework and issued the Transportation Systems Sector (TSS) Cybersecurity Framework Implementation Guidance "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."[109] This guidance

[105] *NIST Cybersecurity Framework (CSF) 2.0* (National Institute of Standards and Technology (NIST), February 26, 2024), https://nvlpubs.nist.gov/nistpubs/CSWP/NIST.CSWP.29.pdf.

[107] NIST Cybersecurity Framework 2.0: Small Business Quick Start Guide (NIST, February 2024), https://csrc.nist.gov/pubs/sp/1300/final.

[108] *NIST Cybersecurity Framework 2.0: Quick Start Guide for Cybersecurity Supply Chain Risk Management (C-SCRM)* (NIST, October, 2024), https://csrc.nist.gov/pubs/sp/1305/final.

[109] *Transportation Systems Sector Cybersecurity Framework Implementation Guidance* (U.S. Department of Homeland Security (DHS), June 26, 2015), 2, https://www.cisa.gov/sites/default/files/publications/tss-cybersecurity-framework-implementation-guide-2016-508v2_0.pdf.

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.[110]

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

Cybersecurity and Infrastructure Security Agency (CISA). CISA was formed in November 2018 with the purpose of building national capacity to defend against cyber-attacks. In addition to its mission to improve protections for federal government computer systems, CISA also develops "trusted partnerships across the public and private sectors" to deliver "technical assistance and assessments."[111]

Looking to improve CISA's cybersecurity influence, in 2021 the Department of Homeland Security established the Cybersecurity Advisory Committee.[112] The Committee works as an independent body to provide recommendations to the CISA Director across the broad spectrum of cybersecurity issues. CISA regularly issues control systems advisories that provide organizations with real-time alerts on security issues, weaknesses, and breaches. Transit agencies are advised to sign up to receive these advisories in case their systems are impacted.

In 2022, CISA released Cross-Sector Cybersecurity Performance Goals[113] (CPGs) after conducting numerous stakeholder meetings with public and private organizations of all sizes to solicit input on how the agency can focus their investment on the most important security outcomes. According to CISA Director Jen Easterly, the CPGs "strive to address this need by providing an approachable common set of IT and OT cybersecurity protections that are clearly defined, straightforward to implement, and aimed at addressing some of the most common and impactful cyber risks."[114] The CPGs are intended to augment the NIST guidelines and provide a "quick start" for agencies looking at where to start on their cybersecurity journey. These performance goals are particularly relevant to small and mid-sized agencies, as they provide a simple starting point for addressing cybersecurity vulnerabilities.

In 2022, CISA also released its Infrastructure Resilience Planning Framework (IRPF), which provides a process and series of resources for incorporating critical infrastructure resilience

[110] *Transportation Systems Sector Cybersecurity Framework Implementation Guidance*, 3.
[111] "ABOUT CISA," Cybersecurity & Infrastructure Security Agency (CISA), accessed August 29, 2024, https://www.cisa.gov/about-cisa.
[112] "Cybersecurity Advisory Committee," CISA, accessed August 13, 2024, https://www.cisa.gov/resources-tools/groups/cisa-cybersecurity-advisory-committee.
[113] CPG Cross-Sector Cybersecurity Performance Goals (CISA, 2022), https://www.cisa.gov/sites/default/files/publications/2022_00092_CISA_CPG_Report_508c.pdf.
[114] "CPG Cross-Sector Cybersecurity Performance Goals," 2.

considerations into planning activities.[115] In 2024, CISA released an updated version (1.2) of the IRPF[116] as well as an IRPF Playbook, which is a how-to guide to assist critical infrastructure stakeholders in executing IRPF guidance to incorporate infrastructure resilience into planning so that communities can become more secure and resilient in the face of multiple threats and changes.[117]

In the updated IRPF, the Agency lays out five key steps to incorporating critical infrastructure resilience into local, regional, and Tribal plans, they are; lay the foundation, identify critical infrastructure, assess risk, develop actions, and implement and evaluate.[118]

CISA also provides a variety of additional tools for transportation agencies, including an Infrastructure Survey Tool (IST) is a voluntary online assessment to both identify and document the security and resilience of a facility or program. The IST combines assessments of risk level and resilience capability to create an overview of facility preparedness. CISA's website also provides access to the National Cyber Security Centre's report on "Best Practices for Event Logging and Threat Detection."[120]

Finally, the agency provides a variety of cyber hygiene services include vulnerability scanning and web application scanning. In its vulnerability scanning offering, the CISA continuously monitors an agency's internet accessible assets for vulnerabilities. Agencies receive a weekly report, as well as ad hoc reports of urgent findings. In its web application offering, CISA scans an agency's web-based applications for vulnerabilities and misconfigurations that a threat actor could exploit. This service provides monthly reports as well as on-demand reports by request. Agencies can sign up for these services for free and start receiving reports within two weeks.

Transportation Security Administration. The 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."[121] Given its provenance, TSA's original orientation centered on physical security, but

[115] "Infrastructure Resilience Planning Framework (IRPF) Version 1.2," CISA, Revision Date, January 24, 2025, accessed March 18, 2025, https://www.cisa.gov/sites/default/files/2024-03/infrastructure-resilience-planning-framework03-22-2024.pdf.
[116] "Infrastructure Resilience Planning Framework (IRPF) Version 1.2."
[117] "Infrastructure Resilience Planning Framework (IRPF) Playbook," CISA, accessed February 10, 2025, https://www.cisa.gov/resources-tools/resources/infrastructure-resilience-planning-framework-irpf-playbook.
[118] "Infrastructure Resilience Planning Framework (IRPF) Playbook."
[120] *Best Practices for Event Logging and Threat Detection* (Australian Government, Australian Signals Directorate's Australian Cyber Security Center (ASD's ACSC), 2024), https://www.cyber.gov.au/sites/default/files/2024-08/best-practices-for-event-logging-and-threat-detection.pdf.
[121] "Mission," Transportation Security Administration (TSA), accessed September 8, 2024, https://www.tsa.gov/about/tsa-mission.

the agency "is responsible for securing the nation's transportation systems from all threats, including both physical and cyber."[122]

In this latter role, the TSA overlaps with CISA. The 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.[123]

The TSA has issued Cybersecurity Directives for multiple TSS entities whose standards and requirements can vary depending on the type, size, and funding of the agency. One Directive that is applicable to several larger transit agencies that include rail is the TSA Security Directive SD 1582-21-01C: Enhancing Public Transportation and Passenger Railroad Cybersecurity.[124] This Directive applies to transit operators that have been designated specifically by the TSA and includes five basic requirements that are the basis for all TSA Security Directives.

Minimum Elements for TSA Security Directives

> Designate a 24/7 cyber security coordinator who must always be available to TSA and CISA to coordinate implementation of cybersecurity practices, manage security incidents, and serve as a principal point of contact with TSA and CISA for cybersecurity-related matters;
>
> 1. Report cyber incidents to CISA within 24 hours;
>
> 2. Develop an incident response plan to reduce the risk of operational disruption should their Information and/or Operational Technology systems be affected by a cybersecurity incident;
>
> 3. Conduct a cybersecurity vulnerability assessment using the form provided by TSA and submit the form to TSA; and

[122] "TSA Releases Cybersecurity Roadmap," TSA, December 4, 2018, accessed August 18, 2024, https://www.tsa.gov/sites/default/files/tsa_cybersecurity_roadmap.pdf.
[123] *TSA Cybersecurity Roadmap 2018* (TSA, November 4, 2018), https://www.tsa.gov/sites/default/files/tsa_cybersecurity_roadmap.pdf.
[124] "Security Directive 1582-21-01C, Enhancing Public Transportation and Passenger Railroad Cybersecurity," TSA, October 24, 2024, https://www.tsa.gov/sites/default/files/security_directive_1582-21-01c_and_memo_508c.pdf.

4. Test a minimum of two objectives from their plan every year which must include employees who have been identified by their positions as active participants in these exercises.

The first four elements are also included in an Information Circular IC-2021-01, *Enhancing Surface Transportation Cybersecurity*, released by TSA December 2021.[125] Unlike the Directive, this document does not expire annually and is not mandatory. It is intended to share information recommendations for improving cybersecurity defenses for surface transportation operations, including railroads, busses, and public transportation agencies that all utilize advanced technology that demands proper security.94

The TSA provides Surface Transportation Resources as a part of their Surface Transportation Cybersecurity Toolkit, including a short list of *Security Resources for Mass Transit Systems*.[126] This one-page document is intended to provide management information to help prevent cybersecurity cyber-attacks in surface transportation operators that employ less than 1,000 staff members. The Toolkit provides links and descriptions to crucial resources for transportation systems, such as the Baseline Assessment for Security Enhancement (BASE), pocket-sized guides on topics such as counterterrorism, contact information for agencies to request access to free services through the Information Sharing and Analysis Center (ISAC), Ransomware Guides, Insider Threat Mitigation, and APTA's Cybersecurity Considerations for Public Transit.

Additional DHS Programs for Public Transit Agencies

Working together, CISA and TSA have established several additional tools to provide outreach and support to transit agencies. One key program is the Cybersecurity Advisors (CSAs) Program. CSAs are DHS personnel assigned to ten regions throughout the United States, corresponding to the Federal Emergency Management Agency's (FEMA) geographic regions. They are responsible for cultivating partnerships with critical infrastructure entities, including passenger rail operators, and providing direct assistance to those entities to promote cybersecurity preparedness, risk mitigation, and incident response capabilities.[127]

[125] "Enhancing Surface Transportation Cybersecurity," IC-2021-01, TSA, December 31, 2021, https://www.tsa.gov/sites/default/files/20211201_surface-ic-2021-01.pdf.
[126] *Security Resources for Mass Transit Systems* (TSA, n.d.), accessed August 21, 2024, https://www.tsa.gov/sites/default/files/tsa_mtpr_resources_slick_sheet.pdf.
[127] *Cybersecurity Advisor* (Department of Homeland Security (DHS), 2017), https://www.bu.edu/tech/files/2017/09/DHS_CSA_Fact_Sheet_2017-1.pdf.

CSA SERVICES – Cybersecurity Advisors

1. Cyber Preparedness: On-site meetings to promote best practices.

2. Strategic Messaging: Briefings, keynotes, and panel discussions to help improve cybersecurity awareness and cybersecurity posture.

3. Working Group Support: Assisting stakeholders in existing information sharing cybersecurity initiatives.

4. Partnership Development: Building local and regional cybersecurity private–public partnerships.

5. Cyber Assessments:

6. Cyber Infrastructure Survey Tool (C-IST): Survey focused on over 80 cybersecurity controls in five key areas, resulting in an interactive decision support tool.

7. Cyber Resilience Review (CRR): Strategic evaluation that assesses cybersecurity management capabilities.

8. External Dependency Management (EDM): Assessment of the management activities and practices utilized to identify, analyze, and reduce risks arising from third parties.

9. Incident Coordination and Support: Facilitating cyber incident response in times of increased threat, disruption, and attack.[128]

4.3 U.S. Department of Transportation

Over the past four years, the U.S. DOT has taken a more active role in addressing its cybersecurity needs as well as those of the agencies that receive federal funding. To coordinate its efforts, the U.S. DOT has established the Office of Sector Cyber Coordination under the Office of the Chief Information Officer.[130] The Office leads coordination, support, and engagement within the U.S. DOT and its operating administrations, as well as with U.S. DOT's regulated community, on

[128] "Cybersecurity Advisor."

[130] "Office of the Chief Information Officer," DOT, accessed September 22, 2024, https://www.transportation.gov/cio.

transportation systems sector cybersecurity matters. Like TSA and CISA, the Office of Cyber Coordination provides an excellent website with a list of available resources.[131]

The U.S. DOT is attempting to make cybersecurity investments for its grant recipients easier. On its website, the FTA clarifies that certain formula grant funding (i.e., Urbanized Area Formula Grant Program, Formula Grants for Rural Areas, State of Good Repair Grant Program) may be used to address certain cybersecurity needs and specifies the expenses they can be used for.[132]

Cybersecurity Costs Eligible Under Formula Grant Programs

- Staff salaries for personnel involved with security, contracts for security services, and other operating activities intended to increase the security of an existing or planned public transportation system.
- Capital costs to support equipment including computer hardware and software to address cybersecurity.

> The Urbanized Area Formula Grant Program makes federal resources available to urbanized areas and governors for transit capital and operating assistance and for transportation-related planning in urbanized areas.

In fact, the Urbanized Area Formula requires that a grant recipient must spend at least one percent of its grant award on security projects, unless the grant recipient determines this is not necessary. However, the Urban Area Formula does not specify whether or how much of these funds must be spent on cybersecurity. While potentially valuable, without additional funding for cybersecurity and a specific mandate, cybersecurity investments must compete with other needs.

The U.S. DOT has been more forceful with discretionary grant programs and now requires all new discretionary grant program recipients to have a cybersecurity program in place or put one in place before receiving funding.[133] The Office of Sector Cyber Coordination works with U.S. DOT's grant program offices to include Critical Infrastructure Security and Resilience language in Notices of Funding Opportunity (NOFO) announcements. An example of this language can be found in the Fiscal Year 2023 SMART Stage 1 Notice of Funding Opportunity:

[131] "Office of Sector Cyber Coordination," DOT, accessed September 22, 2024, https://www.transportation.gov/mission/office-secretary/office-chief-information-officer/office-sector-cyber-coordination.

[132] "Office of Research, Innovation and Demonstration," FTA, accessed July 8, 2024, https://www.transit.dot.gov/regulations-and-programs/safety/cybersecurity-resources-transit-agencies.

[133] "Office of Chief Information Officer." See also "Strategic Objective 3.4: Use Federal Grants and Other Incentives to Build in Security," in *National Cybersecurity Strategy* (The White House, 2023) 21, https://www.whitehouse.gov/wp-content/ uploads/2023/03/National-Cybersecurity-Strategy-2023.pdf.

> It is the policy of the United States to strengthen the security and resilience of its critical infrastructure against both physical and cyber threats, consistent with Presidential Policy Directive 21 - Critical Infrastructure Security and Resilience and the National Security Memorandum on Improving Cybersecurity for Critical Infrastructure Control Systems. Each applicant selected for Federal funding under this notice must demonstrate, prior to the signing of the grant agreement, effort to consider and address physical and cybersecurity risks relevant to the transportation mode and type and scale of the project. Projects that have not appropriately considered and addressed physical and cybersecurity and resilience in their planning, design, and project oversight, as determined by the Department and the Department of Homeland Security, will be required do so before receiving funds or will be required to complete related actions as part of the project.[134]

The U.S. DOT's website also states that grant recipients can expect to be required to implement the four basic requirements outlined in the TSA Information Circular IC-2021-01, Enhancing Surface Transportation Cybersecurity,[135] referenced above.

This language could have a meaningful impact on those transit agencies that receive discretionary grants, many of which do not have basic cybersecurity programs in place. This assumes, however, that the grant recipient is aware of this requirement (anecdotal information indicates that many are not) and that the U.S. DOT is willing to enforce it. Unfortunately, this requirement will not affect many smaller transit agencies that do not have the resources to apply for the U.S. DOT's discretionary grant programs.

4.4 Federal Transit Administration

After September 11, 2001, the FTA developed security and emergency preparedness resources for U.S. transit agencies. Primary among these was the FTA's *The Public Transportation System Security and Emergency Preparedness Planning Guide*,[136] published in January 2003. While this guide does not specifically address cybersecurity, it does provide a helpful structure for preparing for and responding to emergencies, much of which is applicable to cybersecurity. This document later evolved into the *Security and Emergency Preparedness Action Items for Transit Agencies*,[137]which was used by the TSA to develop its voluntary security and emergency preparedness assessment tool, the Baseline Assessment and Security Enhancement (BASE) tool described above. TSA's Surface

[134] "SMART Stage 1 Notice of Funding Opportunity (NOFO)," DOT, August 25, 2023, 30, https://www.transportation.gov/sites/dot.gov/files/2023-08/Final%20SMART%20FY23%20Stage%201%20NOFO_0.pdf.

[135] TSA, IC-2021-01, "Enhancing Surface Transportation Cybersecurity."

[136] *The Public Transportation System Security and Emergency Preparedness Planning Guide* (FTA, January 2003), https://www.transit.dot.gov/sites/fta.dot.gov/files/docs/PlanningGuide.pdf.

[137] Kevin L. Chandler, Jodi M. Rizek, and Pamela J. Sutherland, *Security and Emergency Preparedness Action Items for Transit Agencies* (FTA, September 2014), https://www.transit.dot.gov/sites/fta.dot.gov/files/docs/508_new_top_17.pdf.

Transportation Security Inspector (STSI) function uses the BASE checklist to work with transit agencies on a voluntary basis to complete a programmatic assessment of security and emergency preparedness programs. The main change relevant to this study was the addition of cybersecurity as a topic.[138]

The FTA conducts mandatory reviews of all Urbanized Area Formula Program (5307) grant recipients every three years (Triennial Review). The reviews cover up to 23 areas ranging from Americans with Disabilities Act (ADA) requirements to maintenance standards. Because of the focus on urbanized areas, most small and rural transit agencies are not subject to this review.

In 2024, the FTA revised its Triennial Review manual to include cybersecurity requirements related to transit rail. This section requires that transit agencies that operate fixed rail guideway transit services to certify that they have a process in place to "develop, maintain, and execute a written plan for identifying and reducing cybersecurity risks."[139] Agencies are directed to follow the cybersecurity standards set by NIST. This requirement applies to all operations of the covered transit operation, not just the rail portion of the system. Unfortunately, the FTA was unable to apply this requirement to all transit agencies. Doing so would have been significant.

The FTA provides an excellent webpage that lists cybersecurity resources available to transit agencies.[140] One important resource is the Cybersecurity Assessment Tool for Transit (CATT), which is a free, NIST-based cybersecurity self-assessment tool for transit agencies.[141] The FTA also supports small, rural and tribal transit agencies through a variety of means. Most relevant are:

- **National Rural Transit Assistance Program (RTAP):** RTAP provides a variety of tools to rural transit agencies such as training modules, webinars, and technical briefs on information applicable to rural and tribal transit including cybersecurity. As listed on their website, their primary focus is "providing materials that assist transit agencies in conducting their own trainings."[142]

- **National Center for Applied Transit Technology (N-CATT):** N-CATT was established to provide "small-urban, rural, and tribal transit agencies with practical resources for replicable technological solutions and innovations,"[143] including cybersecurity. The homepage of their website is organized by sections "Tech University," "Technology

[138] Chandler, Rizek, and Sutherland. *Security and Emergency Preparedness Action Items for Transit Agencies*, 8.
[139] *Contractor, Manual, Fiscal Year 2024* (FTA, FY 2024),https://www.transit.dot.gov/sites/fta.dot.gov/files/2024-03/Fiscal-Year-2024-Contractor-Manual_0.pdf.
[140] "Cybersecurity Resources for Transit Agencies," FTA, accessed September 22, 2024, https://www.transit.dot.gov/regulations-and-programs/safety/cybersecurity-resources-transit-agencies#:~:text=Cybersecurity%20is%20now%20a%20component,both%20physical%20and%20cyber%20threats.
[141] "Cybersecurity Assessment Tool for Transit," FTA, updated June 21, 2023, accessed August 29, 2024, https://www.transit.dot.gov/research-innovation/cybersecurity-assessment-tool-transit-catt.
[142] "National RTAP FAQs," National Rural Transit Assistance Program, accessed September 8, 2024, https://www.nationalrtap.org/About/National-RTAP-FAQ.
143 National Center for Applied Transit Technology (N-CATT), accessed September 8, 2024, https://n-catt.org/.

Toolbox," "Events," and "News," all of which lead to specific resources that can be utilized by smaller-scale transit agencies.

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

National Highway Traffic Safety Administration (NHTSA) leads the vehicle cybersecurity research that seeks to prevent attacks on vehicles and components. For example, in 2022, NHTSA published Cybersecurity Best Practices for Modern Vehicles.[144] This Best Practices document is applicable to vehicle Original Equipment Manufacturers (OEMs) but can be a relevant resource to transit operators when purchasing new vehicles as a means of ensuring that they are aware of the types of cybersecurity protections bus manufacturers should be building into their vehicles.

Federal Highway Administration (FHWA) provides formula grant funding to State DOTs to help support qualifying small and rural transit organizations. State DOTs oversee transit systems in small urban (Section 5307) and rural communities (Section 5311), as well as transit providers who serve individuals with disabilities and seniors (Section 5310). FHWA leads the research that seeks to protect the nation's roadside equipment, devices, and systems. In cooperation with the National Highway Institute and other engineering organizations, FHWA developed a handbook entitled the *Federal Highway Administration Cybersecurity Handbook*[145] and provides various resources to state DOTs to help mitigate cybersecurity risk and improved cybersecurity resilience.

In 2024, the FHWA announced that it would be adopting a CISA-developed Cyber Security Evaluation Tool (CSET) with the intention of enhancing protection of transportation infrastructure. CSET is a voluntary desktop software tool that provides a "systematic, disciplined, and repeatable approach to evaluating an organization's security posture."[146]

[144] *Cybersecurity Best Practices for Modern Vehicles* (National Highway Traffic Safety Administration (NHTSA), updated September 2022), https://www.nhtsa.gov/sites/nhtsa.gov/files/2022-09/cybersecurity-best-practices-safety-modern-vehicles-2022-tag.pdf.

[145] *Federal Highway Administration (FHWA) Cybersecurity Program (CSP) Handbook* (Federal Highway Administration (FHWA), December 2017), https://www.fhwa.dot.gov/legsregs/directives/orders/csp_handbook.pdf.

[146] "Notices," *Federal Register* 89, no. 175 (September 10, 2024), https://www.govinfo.gov/content/pkg/FR-2024-09-10/pdf/2024-20331.pdf.

CSET Components[147]

- Designed to help organizations evaluate their cybersecurity practices, identify vulnerabilities, and prioritize mitigation efforts.

- Provides a systematic approach to assess cybersecurity controls and processes.

- Provides a range of modules and questionnaires specific to variety of critical infrastructure divisions.

- CSET v12 includes the Incident Management Review (IMR) which aims to improve cyber resilience via improved overall incident management function.

Intelligent Transportation Systems Joint Program Office (ITS JPO), which was once part of FHWA, is now part of the Office of the Assistant Secretary for Research and Technology (situated in the Office of the Secretary). The ITS JPO is responsible for conducting research into cybersecurity mitigation for transportation technologies and promoting "security by design" for existing and emerging transportation systems.[149] This focus, while important, centers on the transportation technologies themselves, rather than the agencies' processes and procedures for acquiring and operating those technologies.

In 2018, the ITS JPO issued *Cybersecurity and Intelligent Transportation Systems: A Best Practices Guide*,[150] which presents best practices for state and local governments to develop their own ITS cybersecurity plan and penetration test program.

In 2020, the ITS JPO released *ITS JPO Strategic Plan 2020–2025,* which defines its mission as leading "collaborative and innovative research, development, and implementation of intelligent transportation systems to improve the safety and mobility of people and goods."[151] One of the goals in this plan is that "the vulnerabilities that ITS deployments create in the transportation system

[147] Anna Ribero, "FHWA adopts cybersecurity evaluation tool to enhance transportation infrastructure protection," Industrial Cyber, September 13, 2024, https://industrialcyber.co/transport/fhwa-adopts-cybersecurity-evaluation-tool-to-enhance-transportation-infrastructure-protection/.

[149] "Cybersecurity" U.S.DOT Intelligent Transportation Systems, Joint Program Office, access date March 18, 2025https://www.its.dot.gov/resources/Cybersecurity/

[150] Cory Krause, Justin Anderson, Kellen Shain, Linda Nana, Tom Mazzone, Stephen McNaught, Mark Jackson, *Cybersecurity and Intelligent Transportation Systems: A Best Practices Guide* (U.S. DOT, September 17, 2019), https://rosap.ntl.bts.gov/view/dot/42461.

[151] "ITS JPO Strategic Plan 2020–2025," Department of Transportation (DOT), Office of the Assistant Secretary for Research and Technology, Intelligent Transportation Systems, Joint Program Office (ITS JPO), May 6, 2020, https://www.its.dot.gov/stratplan2020/ITSJPO_StrategicPlan_2020-2025.pdf.

will be continually and systematically assessed at all levels so that risks associated with malfunction or malfeasance are mitigated to an acceptable level and resiliency plans exist and are in use."[152]

In 2024, the ITS JPO released *Cybersecurity Language for Procurement of Intelligent Transportation Systems*, which provides useful guidance for agencies and model language to consider when drafting contracts with vendors.[153]

4.5 Corollary State Agencies

Every state has a corollary to DHS in some form. Most have technology hubs (e.g., office of the Chief Information or Technology Officer). These can also serve as resources for public transit agencies to support their cybersecurity efforts. The National Guard is also beginning to take an active role. Examples of state-level National Guard commissions can be found in the 2020 Study.[154]

Industry Associations Supporting Transit Cybersecurity[155]

As with many aspects of the U.S. economy, much of the onus for ensuring effective management of cybersecurity risks rests within the industry itself. Much of this work occurs through national and state industry associations. The most prominent national associations impacting transit in the United States include:

The American Public Transportation Association (APTA). APTA is an international trade association with more than 1,500 public and private sector members. APTA provides a broad range of services to its members that include advocacy and policy, standards, guidance and best practices, training, research, and technical support.

APTA provides much of its cybersecurity guidance through its Security Standards Policy and Planning Committee and its working groups on security and emergency management standards. The Security Standards Policy and Planning Committee is composed of representatives from several prominent transit organizations and businesses and is organized into several working groups.

[152] "ITS JPO Strategic Plan 2020–2025," 32.

[153] Dan Lukasik, Jack Oden, Robert Sanchez, Brian Russell, Kyle Rush, and Adam Chandler, "Cybersecurity Language for Procurement of Intelligent Transportation Systems, ITS" DOT, January 22, 2024, https://rosap.ntl.bts.gov/view/dot/73792.

[154] Belcher

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

One important working group is the Enterprise Cyber Security working group that has produced several valuable resources for transit agencies. In 2022, the Enterprise Cyber Security Working Group updated their Cybersecurity Considerations for Public Transit.[156] APTA relied on the original NIST Cybersecurity Framework as the guidance that transit agencies can and should base their cybersecurity practices upon.

This Recommended Practice identifies the human element of a cybersecurity program as its weakest link, and outlines three ways in which this link can be strengthened:

- **Education** is a crucial step to increasing confident and capable cybersecurity personnel. Employees should possess the capacity to demonstrate full understanding of the cybersecurity practices and standards that their company is implementing to ensure that there is little confusion when it comes to protecting employee and customer data.

- **Training** should be enforced to increase security skill sets and knowledge within the workplace. Though they intersect, the key difference between training and awareness is that "training seeks to teach skills that allow an individual to perform a specific function at a certain level of competency, while awareness seeks to focus an individual's attention on an issue or a set of issues."

- **Awareness** promotes security and accountability. This can be achieved through communication, outreach, and metrics development.[157]

The Enterprise Cyber Security Working Group also produced *Enterprise Cybersecurity Training and Awareness*, which provides information that transit agencies can use to begin building cybersecurity training and awareness programs.[158] Finally, in 2024, APTA released an update to its 2019 training video for transit executives called *Cybersecurity Fundamentals for Senior Executives*.[159] APTA also provides an excellent webpage referencing relevant resources for transit operators.[160]

The Community Transportation Association of America (CTAA). CTAA has worked with 52 communities through both federal and non-federal Technical Assistance Centers, providing specific training for customer demands. The association includes 1,200 members, affiliates, and

[156] Enterprise Cyber Security Working Group, "Cybersecurity Considerations for Public Transit," American Public Transportation Association (APTA), updated July 29, 2022, accessed October 21, 2024, https://www.apta.com/wp-content/uploads/APTA-SS-ECS-RP-001-14_R1.pdf.

[157] Enterprise Cyber Security Working Group, "Cybersecurity Considerations for Public Transit," 14.

[158] "Enterprise Cybersecurity Training and Awareness," APTA, March 27, 2019, accessed July 8, 2024, https://www.apta.com/research-technical-resources/standards/security/apta-ss-ecs-rp-002-19/.

[159] APTA, "Cybersecurity Fundamentals for Senior Executives," (video), November 7, 2024, accessed November 7, 2024, https://learning.aptagateway.com/products/cybersecurity-fundamentals-for-executives.

[160] "Cybersecurity Resources," APTA, accessed, July 8, 2024, https://www.apta.com/research-technical-resources/safety-security/cybersecurity-resources/.

individuals.[161] Among the many services that CTAA provides its members, it regularly provides educational sessions on cybersecurity, often in conjunction with RTAPP or N-CATT. Beginning in 2024, CTAA partnered with a private company, Cybrbase, to provide low-cost cybersecurity assessments to its members.

The Transportation Research Board (TRB). The TRB is a part of the National Academies of Sciences, Engineering, and Medicine, and serves to mobilize "expertise, experience, and knowledge to anticipate and solve complex transportation-related challenges.[162] Through numerous programs and divisions, the TRB engages in work with consumers and team members as individuals at the volunteer level, all the way up to the U.S. Congress and executive branch to produce research, information exchange forums, and fellowship programs.

The TRB manages the Transit Cooperative Research Program (TCRP) that develops near-term, practical solutions to problems facing public transportation. TCRP is sponsored by the FTA and works in partnership with APTA.

In 2022, TCRP produced *Cybersecurity in Transit Systems.*[163] The report focuses on the impact of the global pandemic and discusses emerging cybersecurity trends related to teleworking/remote worker offices, contactless customer services, real-time information services, transit-on-demand services, and cyber resilience affecting transit agencies now and in the future.

TRB also manages the National Cooperative Highway Research Program (NCHRP) which produces systematic, well-designed, and implementable research to help solve problems facing state departments of transportation administrators and engineers.[164] NCHRP is funded by participating member states of the American Association of State and Highway Transportation Officials (AASHTO) and FHWA. In 2020, NCHRP released NCHRP Research Report 930: *Update of Security 101: Developing a Physical and Cyber Security Primer for Transportation Agencies*[165] This report provides transportation managers and employees with an introductory-level reference document to enhance their working knowledge of security concepts, guidelines, definitions, and standards. It covers the major components of an effective security program at the conceptual level, including risk management and risk assessment, plans and strategies, security countermeasures,

[161] *Strategic Plan 2021–2025* (Community Transportation Association of America (CTAA)), accessed September 15, 2024, https://ctaa.org/wp-content/uploads/2021/09/CTAA-Strategic-Plan-FInal-1.pdf.

[162] "About | Transportation Research Board," National Academies, accessed September 15, 2024, https://www.nationalacademies.org/trb/about.

[163] *Cybersecurity in Transit Systems* (National Academies of Science, Engineering, and Medicine, 2022), https://doi.org/10.17226/26475

[164] "National Cooperative Highway Research Program (NCHRP)," Transportation Research Board (TRB), accessed September 15, 2024, https://www.trb.org/NCHRP/NCHRP.aspx

[165] *Developing a Physical and Cyber Security Primer for Transportation Agencies* (National Academies of Science, Engineering and Medicine, 2020), https://doi.org/10.17226/25869.

cybersecurity, workforce planning and training/exercises, infrastructure protection and resilience, and homeland security laws, directives, and guidance.

American Association of Highway and Transportation Officials (AASHTO). AASHTO represents the state highway and transportation departments in the 50 states, the District of Columbia, and Puerto Rico. It represents all transportation modes and serves as a liaison between state departments of transportation and the federal government.

State DOTs have multimodal responsibility, and as a result, AASHTO has a Council on Public Transportation to meet the needs of the staff supporting transit agencies that receive federal funding through the states. This Council "develops legislative, policy, and program recommendations related to all forms of passenger public transportation services."[166] AASHTO also provides its members educational sessions on cybersecurity, often in conjunction with the Multi-State Transit Technical Assistance Program (MTAP), which it supports. The primary purpose of MTAP is to provide technical assistance to help states implement FTA programs, to provide feedback to FTA on implementation issues, and to create a professional network for sharing best practices.[167]

Intelligent Transportation Society of America (ITS America). ITS America is a multi-stakeholder trade association that advocates for transportation innovation within the United States. ITS America focuses its work on cybersecurity though its Cybersecurity Community of Practices.

In 2024, ITS America published a Cybersecurity Issue Brief entitled "Is Cybersecurity a Core Safety Issue for Transportation?" The Brief outlines the connection between Operational and Information Technology, as well as security procedures and best practices for both OT and IT. It concludes that "these best practices must be incorporated at the beginning of the lifecycle of connected transportation infrastructure projects and should represent the byproduct of close collaboration among private sector technology developers, public sector technology deployers, and Federal security practitioners."[168]

[166] "Council on Public Transportation," American Association of State Highway Transportation Officials (AASHTO), accessed October 12, 2024, https://transportation.org/ptc/.

[167] "Council on Public Transportation."

[168] John Contestabile, Paul Lennon, Christopher Lyons, and Rick Tiene, "Issue Brief: Cybersecurity; Is Cybersecurity a Core Safety Issue for Transportation?" (Intelligent Transportation Society of America (ITS America), July 2024), https://itsa.org/wp-content/uploads/2024/07/Cybersecurity-and-Transportation-Safety-Issue-Brief-Final-Version.pdf.

5. Key Findings

The findings that follow are based primarily on the results of the survey, with additional context from interviews conducted by the authors as well as applicable literature. Not every specific type of transit was represented in the survey responses, but there is enough variety and a broad distribution of agencies across mode, size, urbanization level, and region that the authors believe this sample is representative. The authors also believe that because of this distribution, statistically significant conclusions can be drawn based on the data, especially in cases where trends are strong and differences are large.

Finding 1: There is a Lack of Organizational Knowledge About Cybersecurity

The first theme from the research is that much of the transit industry still demonstrates a lack of organizational knowledge about cybersecurity. Many executives do not appreciate the cybersecurity risks their organizations face, and if they do, many do not know what their teams are doing to address these risks. These patterns revealed themselves through the data gathered on cybersecurity assessments, training, and staffing.

5.1 Cybersecurity Assessments

A cybersecurity assessment is one of the most important tools an agency can deploy to reduce their cyber risk and improve their overall cyber resiliency. A cybersecurity assessment allows an agency to pinpoint its vulnerabilities, align with best practices, determine where it is falling behind, and prioritize responses. While there are many effective tools that transit agencies can use to execute a cybersecurity assessment, there are also several basic, free tools, which any transit agency can and should use, including the Cyber Resilience Review (CRR) developed by CISA and based on the NIST Cybersecurity Framework, and the FTA's CATT tool, also based on the NIST Cybersecurity Framework. While TSA recommends completing a cybersecurity vulnerability assessment, there is no mandate for most transit agencies or required frequency. General best practices recommended by CISA suggest that regular, ideally yearly, risk and vulnerability assessments (RVAs) are essential in managing cyber risks across critical infrastructure sectors.[169] Further, engaging an outside organization to facilitate this assessment can help avoid confusion, ensure broad participation, and support accurate responses.

In the survey, the authors asked transit agencies how often they conducted a cybersecurity assessment. The survey also asked agencies to identify which tools they used to conduct the assessments. Of the agencies that responded, over a third said they were not performing annual cybersecurity assessments.

[169] "Cybersecurity Best Practices," CISA, accessed October 22, 2024, https://www.cisa.gov/topics/cybersecurity-best-practices.

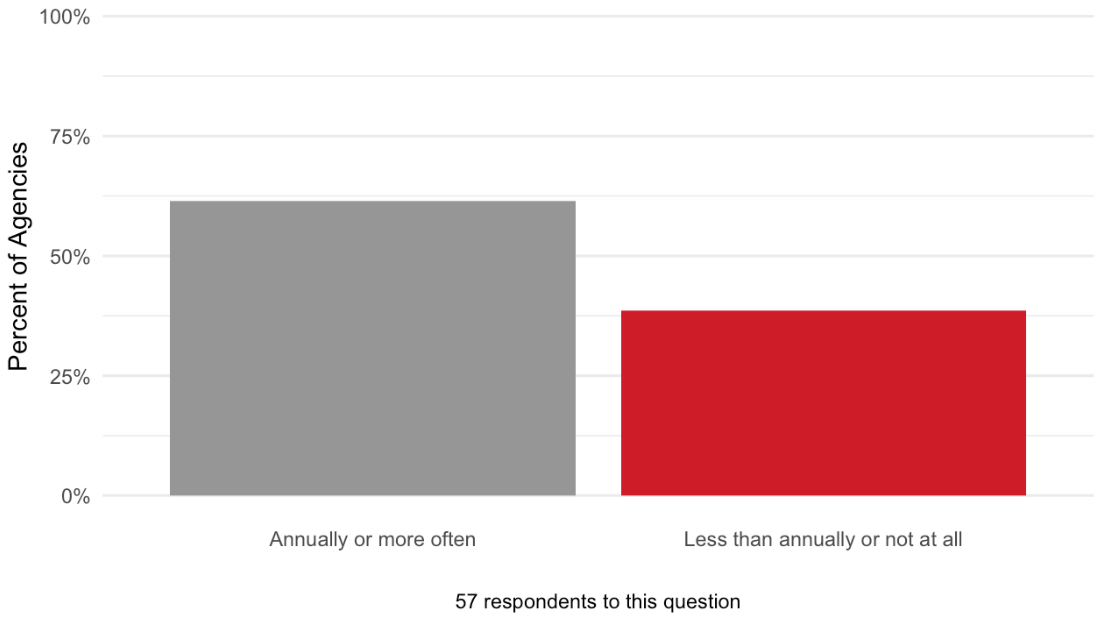


Figure 18. Frequency of Cybersecurity Assessments

Even more concerning, however, is the size of many of the agencies that reported never having completed a cybersecurity assessment. Among these nine agencies, four had operating budgets of more than $30 million in 2022, and one agency had a budget exceeding $100 million. These agencies are large enough to have the minimal internal resources needed to complete a free cyber assessment.

A closer look at the agencies which responded that they conducted annual cybersecurity assessments revealed further issues. Of these agencies, 47% did not know what type of tool they used to conduct their cybersecurity assessment or listed a tool that is not a cybersecurity assessment tool, such as penetration testing tools, network management software, or vulnerability management systems.

Twenty-one percent stated that this task was handled by an external contractor and that they did not know what tool the contractor used. Cybersecurity assessments are designed to be an enterprise-wide exercise where executive leadership from all major departments engage in the assessment process to inform organizational policy. It would be difficult to conduct an effective assessment that engages the entire executive team without knowing which assessment tool was used, even if the assessment was led by a third party.

To reflect this nuance, the respondents were broken into four categories, as seen in Figure 19. The "annual assessment, true assessment tool" category represents those who reported conducting an annual assessment and reported using a recognized cybersecurity assessment tool. These results represent less than a third of the respondents, while the others did not know which tool they used.

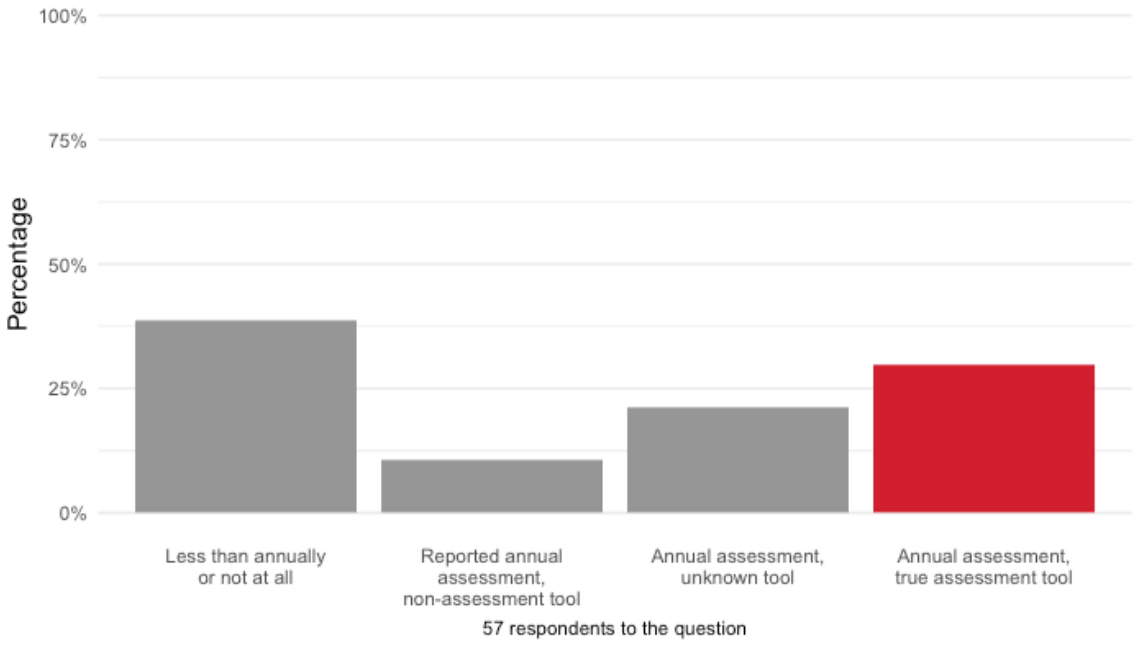


Figure 19. Annual Assessment Responses

This issue is even more pronounced for smaller agencies. As seen in Figure 20, almost half of agencies with operating budgets over $50M conduct annual cybersecurity assessments, while less than a quarter of the agencies with budgets below $50M do so.

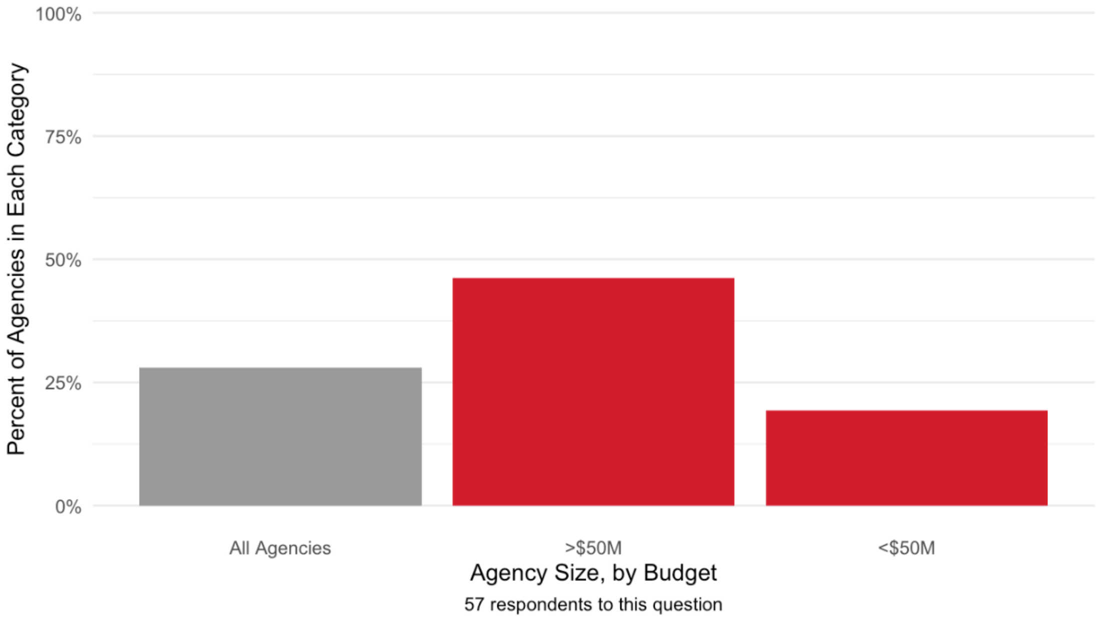


Figure 20. Proportion of Agencies Conducting an Annual Cybersecurity Assessment

5.2 Cybersecurity Staffing and Formal Certifications

Having qualified staff to manage or oversee cybersecurity activities is an important indicator of an agency's appreciation of the significance of cybersecurity to its operations. While many agencies may not be large enough to have dedicated cybersecurity staff, having an IT professional with a cybersecurity certification to oversee cybersecurity operations or contractors can be an indicator that the agency understands the importance of cybersecurity. While almost all agencies with operating budgets above $50M employed at least one full time equivalent (FTE) for cybersecurity, less than half of the agencies in the smallest category did so.

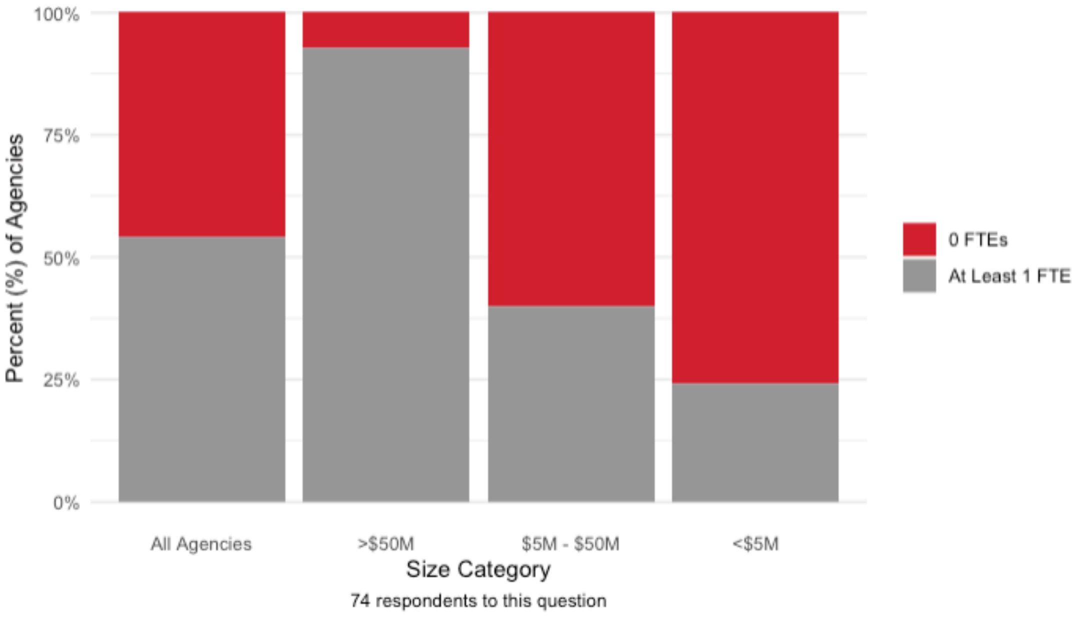


Figure 21. ***Cybersecurity Staffing by Agency*** Size

The difference between large and small agencies is even more pronounced when looking at agencies with employees that have cybersecurity certifications. Cybersecurity certifications require accepted levels of training and studying, as well as demonstrated technical aptitude and knowledge. The purpose of such certification is to ensure a standard level of expertise and allow agencies to ensure that the people who are working on cybersecurity are qualified to do so.[170]

[170] "Why Cyber Security Certifications Matter in Today's World," Thrive DX, June 20, 2024, accessed October 18, 2024, https://thrivedx.com/resources/blog/why-cybersecurity-certifications-matter-in-todays-world-2#:~:text=The%20Value%20of%20Cybersecurity%20Certifications,-Validation%20of%20Skills&text=Cybersecurity%20certifications%20are%20a%20benchmark,data%2C%20and%20prevent%20data%20breaches.

Among the agencies who responded to both the 2020 and the 2024 survey, the percentage of agencies with certified cybersecurity professionals decreased from 53% to 44%. Based on the data, it is not possible to determine what fueled this change.

Of the agencies surveyed, more than 60% did not have a person on staff with a cybersecurity qualification of any kind. This is not surprising given that most of these agencies also reported not having any full-time employees working exclusively on cybersecurity. What is surprising is that almost 30% of the agencies who reported having at least one FTE dedicated to cybersecurity also reported having no staff members with a cybersecurity certification. Two agencies reported having nine to fifteen full-time employees working on cybersecurity, yet none of them had any cybersecurity certifications.

Analyzing differences in agency size, in combination with agency interviews, reveals that this problem is likely linked to a lack of resources. Most of the largest agencies in the sample, those with budgets above $50M, have employees with cybersecurity certifications, while almost none of the agencies with budgets below $5M have any employees with cybersecurity certifications. Many of these smaller agencies also do not have dedicated IT staff and outsource their IT support and/or have a person on their team "that is good with computers."

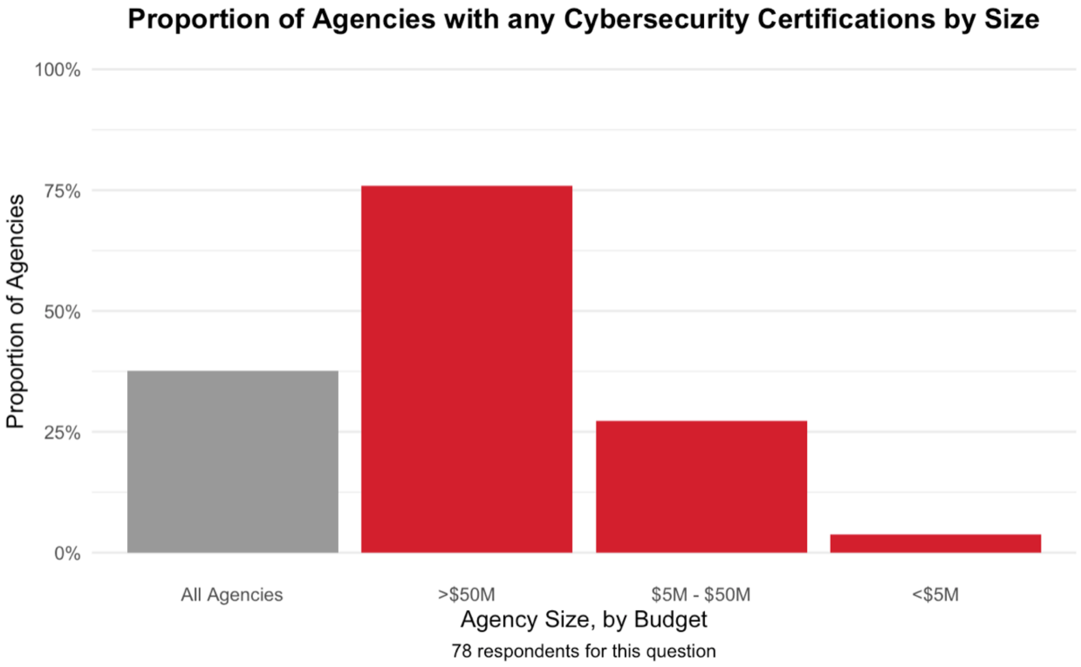


Figure 22. Proportion of Agencies with any Cybersecurity Certifications by Size

5.3 Cybersecurity Training

While cybersecurity certifications are important for cybersecurity and information technology professionals, all employees need to have at least a basic understanding of cybersecurity. Internal cybersecurity training is an important way to ensure that all employees have the knowledge and experience they need to ensure they do not inadvertently cause or allow a cyber breach. While many organizations recommend training as frequently as two or three times a year for all employees,[171] NIST recommends training for all employees at least once a year. Moreover, this training should be differentiated to reflect an employee's role within the organization.

Among the agencies that participated in both the 2020 and 2024 survey, there has been a marked improvement in training rates. While less than half (47%) reported having annual training for all employees in 2020, 83% of the 35 agencies that responded to both surveys now report doing so.

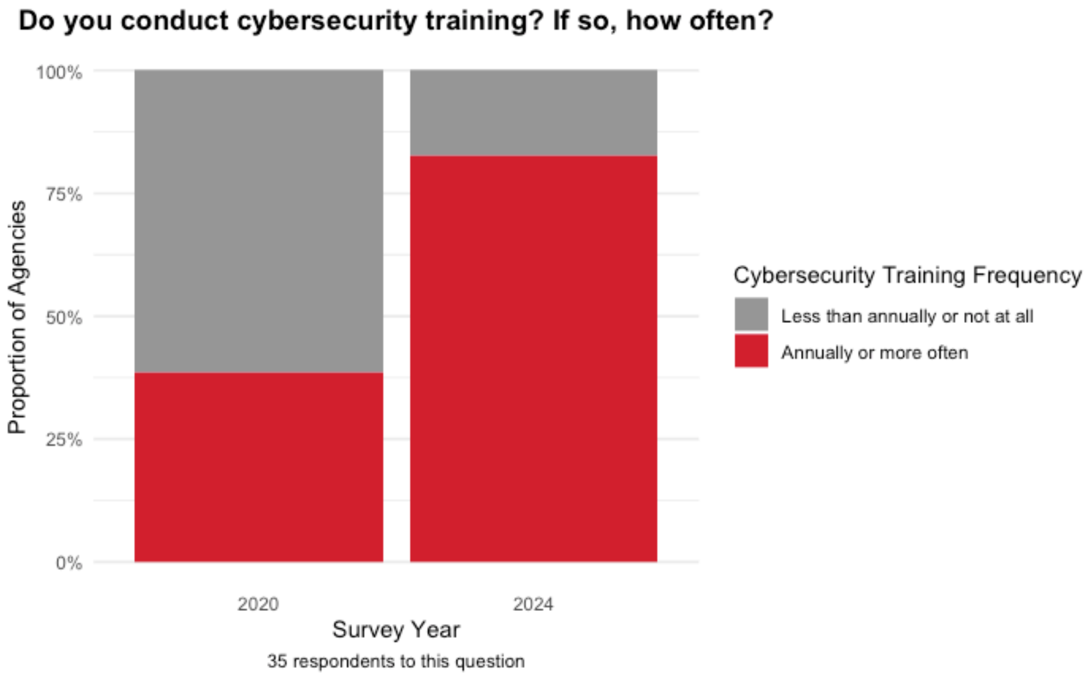


Figure 23. Cybersecurity Training Comparison from 2020 to 2024

While this improvement is positive, the overall data still reveals a troubling picture. When asked whether they conducted cybersecurity training, approximately a third reported that they had never conducted cybersecurity training. Further, roughly 10% reported that they conducted cybersecurity training only sporadically and less than once a year.

[171] Tan Soon Chew, "Considerations for Developing Cybersecurity Awareness Training," ISACA, March 1, 2023, https://www.isaca.org/resources/isaca-journal/issues/2023/volume-2/considerations-for-developing-cybersecurity-awareness-training#:~:text=Frequency%20of%20Training,forget%20what%20they%20have%20learned.

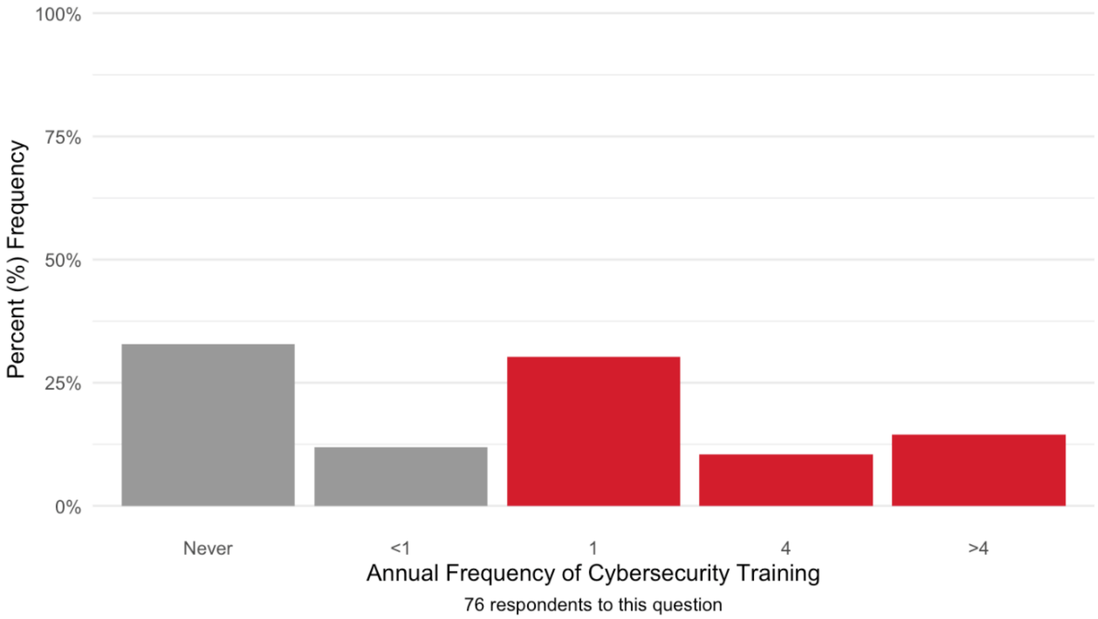


Figure 24. Frequency of Cybersecurity Training by Agency

With cybersecurity training resources broadly available and, in many cases, free,[172] this result suggests that many agencies are not aware of these free resources, do not appreciate the importance of cybersecurity training, or have not prioritized cybersecurity training. In addition, most (56%) of the agencies that reported conducting training did not report differentiation between employees, meaning all employees are receiving the same training.

A significant driver of the difference between the agencies which responded to both surveys and the overall data from the 2024 survey is that small agencies are generally not conducting cybersecurity training. As seen in Figure 25, agencies with budgets above $50M conducted annual training at the highest rate, which was not much higher than the rate among the agencies with budgets between $5M and $50M, both of which were above 75%. The biggest drop-off came for the agencies with budgets below $5M, of which only two of the 26 conduct annual training.

[172] See Section II, Existing Cybersecurity Guidance for Transit.

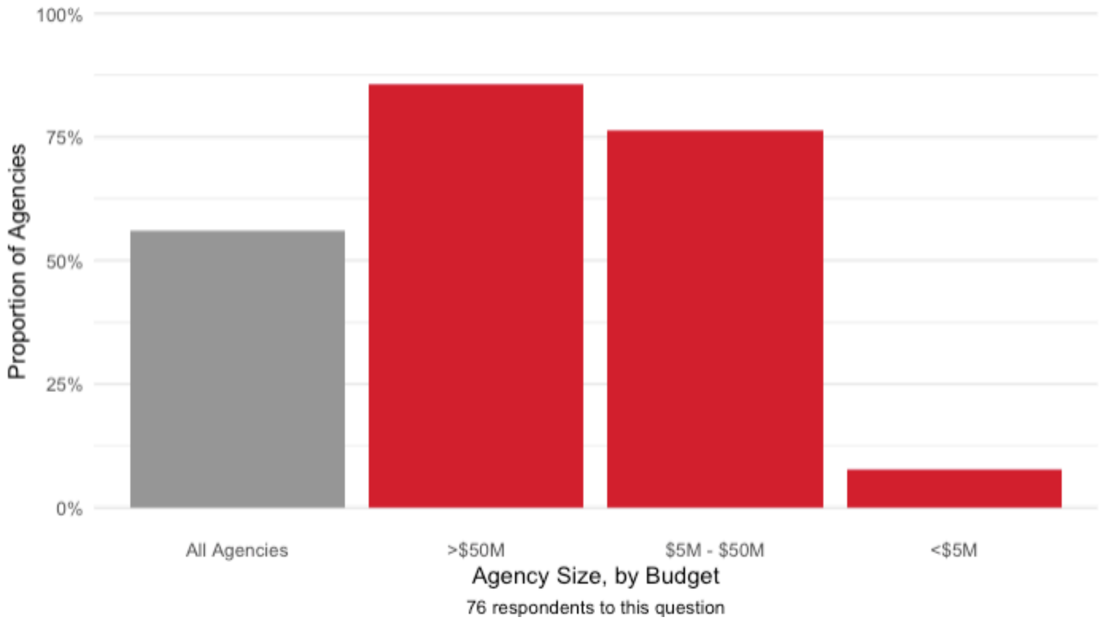


Figure 25. Proportion of Agencies Conducting Cybersecurity Training at Least Annually

Anomalous Survey Responses

The authors included several demographic questions in the survey. Agencies were asked to answer questions about their budgets, employees, and structure. Many agencies provided responses that the authors found anomalous:

Nine agencies reported spending less than $50k on cybersecurity while retaining at least one full-time employee. The average salary for entry-level cybersecurity roles is above $90k,[173] and median benefit costs are almost $30k,[174] which makes this response even less likely. One of these agencies reported having more than eight full time employees working on cybersecurity while spending less than $50k on cybersecurity.

- One agency had a budget of over $1 billion while reporting that they spent less than $50k on cybersecurity.

- Four agencies said that they update their cybersecurity policy at least every year but reported that it had been more than a year since the last update.

[173] Garrett Andrews, "Cybersecurity Salary Guide: How Much Can You Earn?" *Forbes*, updated February 20, 2024, https://www.forbes.com/advisor/education/it-and-tech/cybersecurity-salary-outlook/.
[174] Bureau of Labor Statistics, "Employer Costs for Employee Compensation – December 2024," news release, March 14, 2025, https://www.bls.gov/news.release/pdf/ecec.pdf.

- Thirty-one agencies reported that their budget fell in a category other than the one which corresponded to the data they submitted to the FTA for the NTD database.

- For each of these anomalies, there are plausible answers. For example, it is possible that the questions were not clearly presented. Perhaps the individual responding to the question on behalf of the agency misunderstood the question, relied on outdated information, or was not the correct person to answer the question.

At the very least, these discrepancies demonstrate how hard it is, especially for small agencies, to accurately measure their cybersecurity posture without more guidance and help than they currently receive.

The number of anomalies in the responses, in combination with the findings set out above, suggest that many agencies do not understand or implement these basic best practices. Additionally, some agencies that do so lack a full awareness of the resources and practices they are implementing.

Finding 2: Many Agencies Lack Important Documented Policies and Procedures

To mitigate their cybersecurity risk, agencies must pursue both cybersecurity and cyber resilience, where cybersecurity focuses on attack prevention and cyber resilience focuses on attack response. Within organizations, there are two general channels through which agencies protect themselves from cyberattacks and increase both their cyber resilience and cybersecurity. One channel is with technology or related best practices, which typically focuses on cybersecurity and not on cyber resilience. Penetration testing and endpoint protection tools help agencies find weaknesses in their cyber defenses so that they can patch them. Encryption makes it harder for attackers to access data in transit and at rest in the event of a breach. Firewalls allow control over network traffic and can prevent unwanted intrusions. Vulnerability scans help identify new exploits and out of date software which might allow a cybercriminal to gain access to an agency's systems. None of these technological solutions matter, however, unless agencies have effective, documented policies and procedures in place and are following them.

Firewalls do not matter if an employee unwittingly clicks on a bad link and sends data to an attacker or opens access to the network. Only training and access management policies can prevent that. Effective security controls on systems have no benefit unless they are implemented across the agency's systems without exception. Vulnerability detection software is unreliable unless agency policy mandates swift mitigation of these vulnerabilities. And ultimately, despite an agency's best efforts, many agencies will get hacked. Without an effective incident response plan, as well as other cyber resilience measures, any hack can turn into a disaster.

Because of the importance of such policies and procedures, the authors surveyed the respondents about their adoption of the policies and procedures most critical for these agencies. The responses demonstrated a lack of documented policies and procedures across a broad spectrum of those that are considered by most cybersecurity professionals as essential.

5.4 Cybersecurity Policies

The first deficiency noted was that many agencies lack a documented cybersecurity policy. Such a policy identifies rules and practices for protecting various systems against cyber-attack and provides guidelines for employees on how to minimize cyber risk. Without a cybersecurity policy, employees must make these decisions on their own, resulting in a lack of consistency that can make it much easier for a threat actor to exploit vulnerabilities.

Among the agencies that took both the 2020 and 2024 surveys, there was a moderate increase in the adoption of cybersecurity policies. Even so, approximately a quarter still did not have a cybersecurity policy.

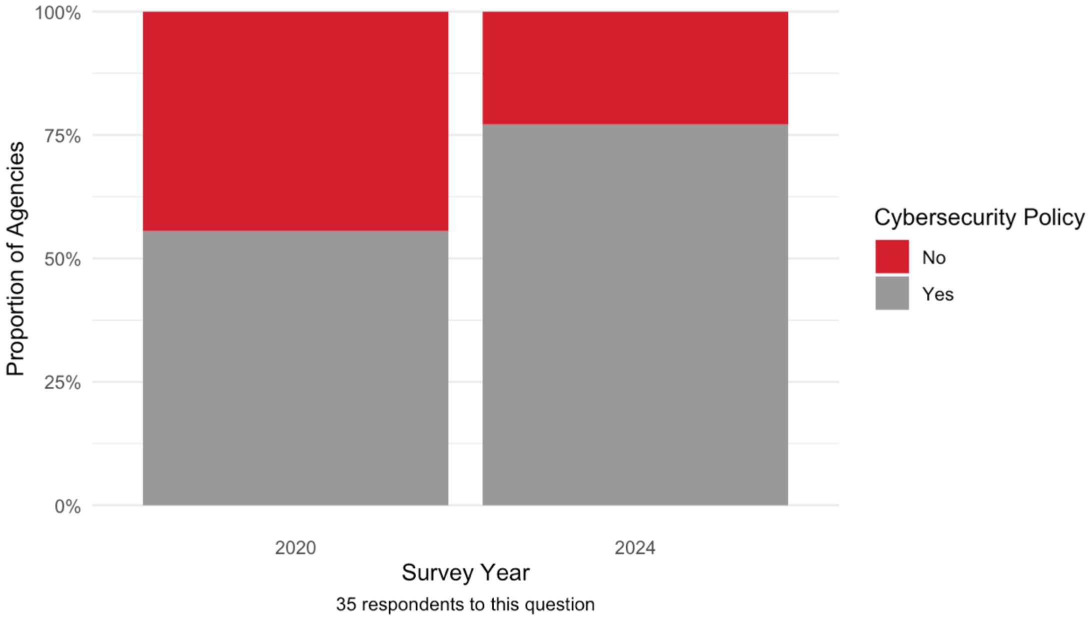


Figure 26. Change in Cybersecurity Policy Adoption from 2020 to 2024

Out of all the agencies surveyed, only 46% had a documented cybersecurity policy. Many of the basic guidelines that a cybersecurity policy should contain are available for free from a variety of government agencies such as NIST and CISA. As such, even small agencies with limited resources should be able to develop a cybersecurity policy at little to no cost.

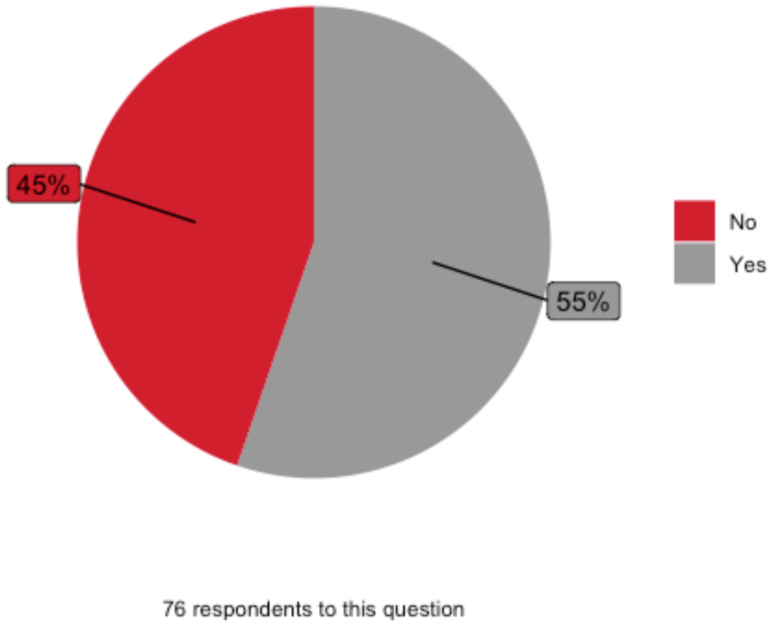


Figure 27. Current Cybersecurity Policy Adoption

As with other policies, adoption is considerably worse for smaller agencies. This is shown in Figure 28.

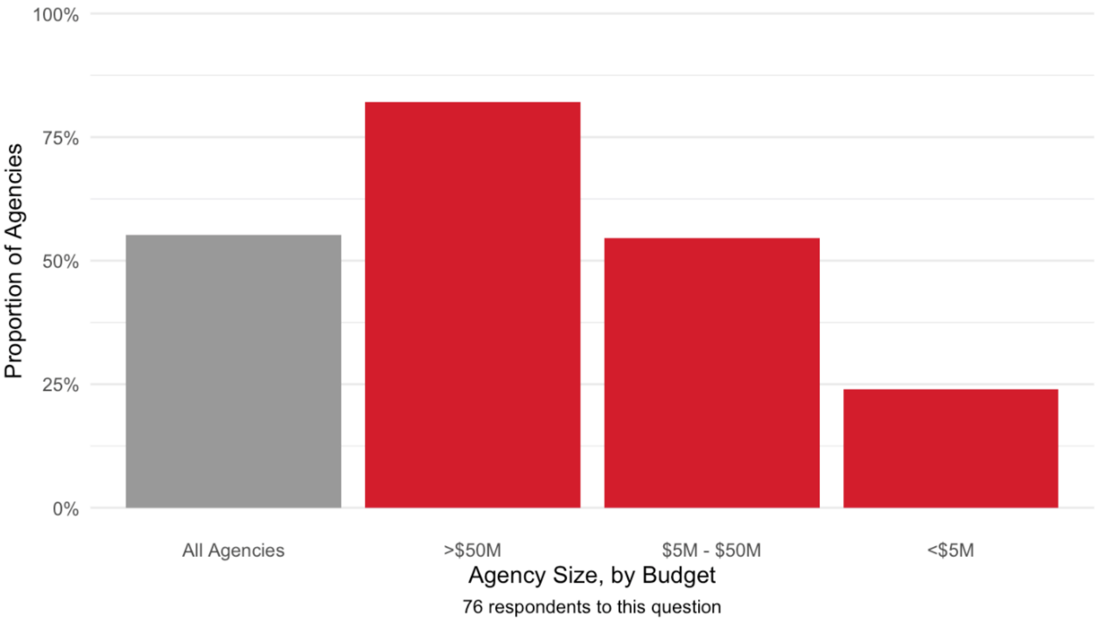


Figure 28. Proportion of Agencies with a Documented Cybersecurity Policy

5.5 Disaster Response Plans

Fundamental to an agency's successful operations is the existence of a documented disaster response plan. A disaster response plan applies to all significant events, including cybersecurity events. A disaster response plan sets guidelines for responding to interruptions, including natural disasters, power outages, communications shutdowns, physical security breaches, and more. Because of the importance of having a disaster response plan, the CISA, FTA, and APTA provide a variety of disaster and emergency response planning resources.

The agencies that responded to both surveys showed strong adoption. A few agencies changed their response, but there was negligible change overall. It is possible, even likely, that those agencies that reported having an incident response plan in 2020, but not in 2024, still have a plan, but the individual responding to the survey did not know this.

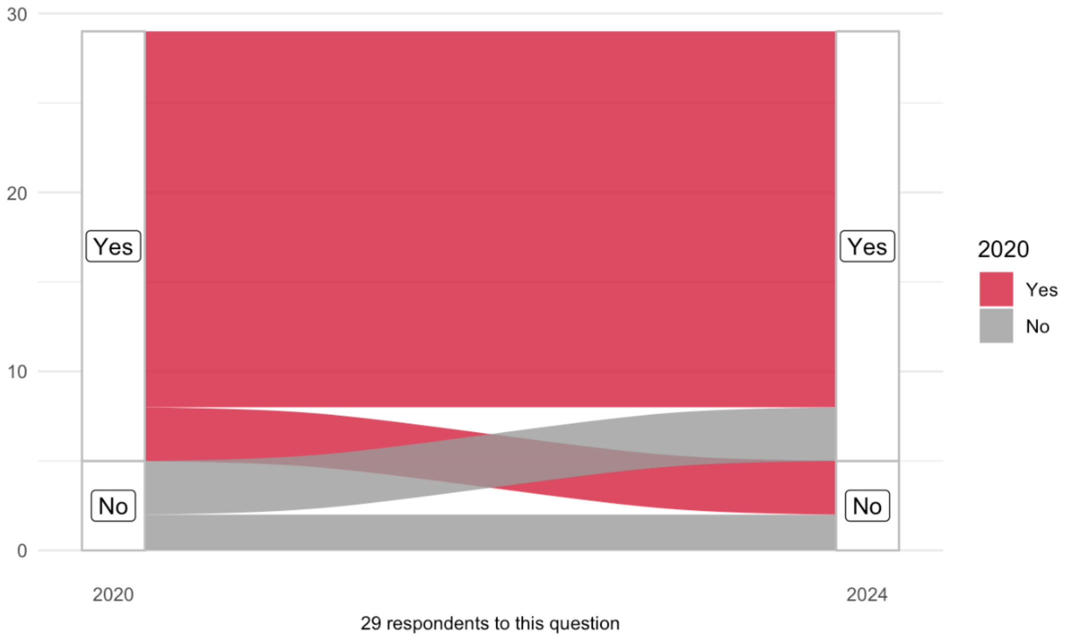


Figure 29. Change in Disaster Response Plan Adoption from 2020 to 2024

For the entire cohort, adoption was moderate. More than a third did not have a disaster response plan.

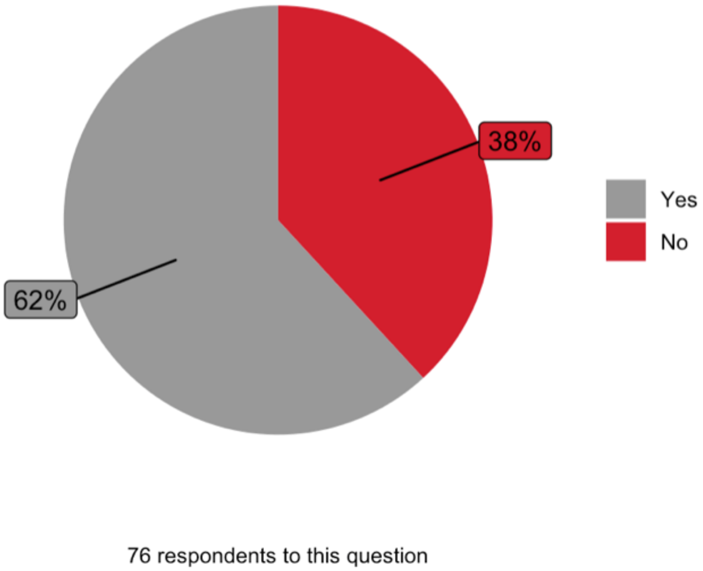


Figure 30. Disaster Response Plan Adoption

This result shows slightly better adherence to this best practice than to the cybersecurity incident response plan discussed below. Moreover, the difference between agencies having budgets greater than $50M and less than $50M was much less severe, suggesting a more widespread understanding and prioritization of the disaster response plan than the cybersecurity incident response plan.

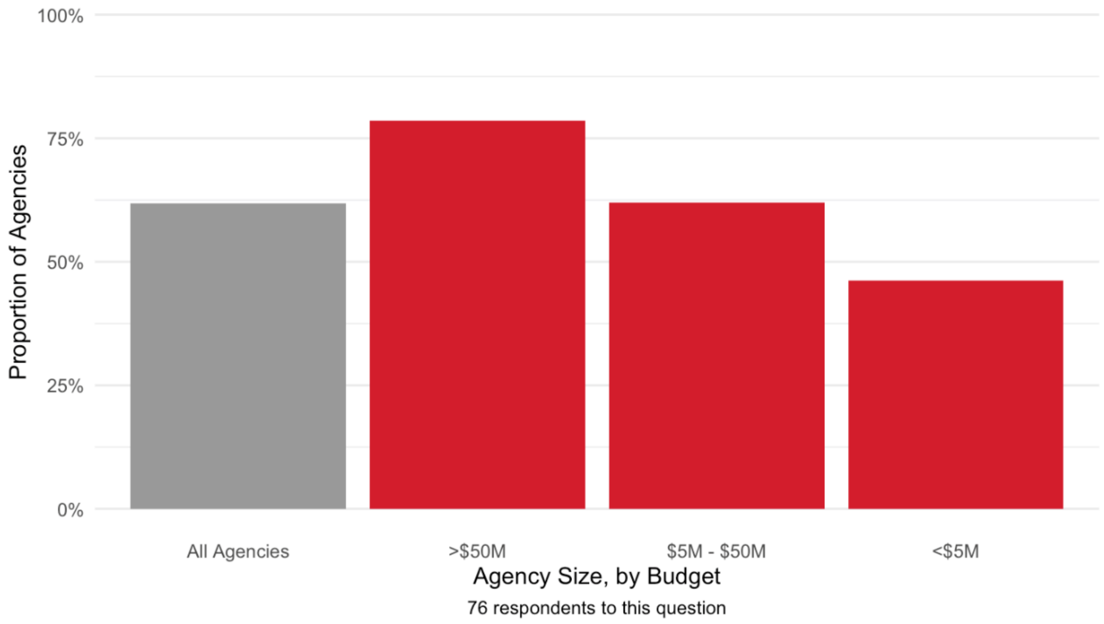


Figure 31. Proportion of Agencies with a Documented Disaster Response Plan

5.6 Cybersecurity Incident Response Plans

Documented cybersecurity incident response plans are a critical tool for all agencies. They outline the actions an agency should take during and after a cybersecurity incident to mitigate its effects and return to normal operation as quickly and safely as possible. Having such a plan allows more effective coordination. It also allows agencies to make difficult decisions regarding the handling of a security incident prior to a real incident, when time is scarce and stress runs high. CISA recommends that organizations have an incident response plan and review it quarterly with all those involved.[177]

For this policy, there was little change among the agencies that answered both surveys. Similar to disaster response plans, a few agencies that did not have a cybersecurity incident response plan as of the last survey now do, and vice versa.

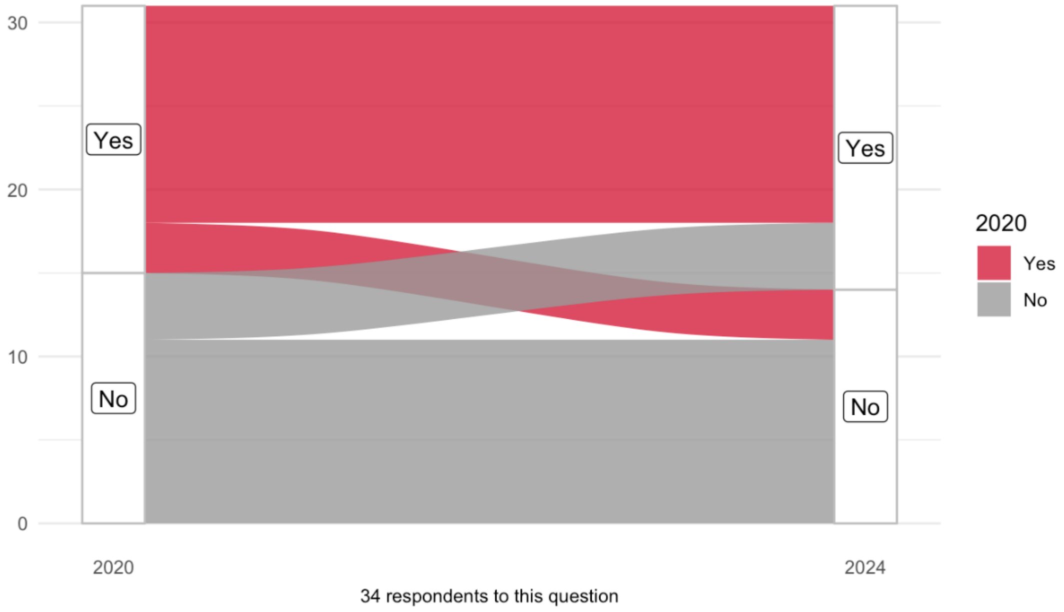


Figure 32. Change in Cybersecurity Incident Response Plan Adoption from 2020 to 2024

[177] "Incident Response Plan (IRP) Basics," Cybersecurity & Infrastructure Security Agency (CISA), accessed October 10, 2024, https://www.cisa.gov/sites/default/files/publications/Incident-Response-Plan-Basics_508c.pdf.

Responding to an Attack Without a Disaster Recovery and Cybersecurity Response Plan in Place Will be More Time Consuming and Costly

> To prevent the spread of a cybersecurity breach through their network, a mid-sized agency that was interviewed took their entire infrastructure offline, physically disconnecting it from the internet. This included critical systems such as CAD/AVL, email, and more. For over two months, the agency operated using manual processes while working to safely restore their infrastructure. Compounding the challenge, they had no Disaster Response or Business Continuity Plans to guide their efforts, which could have made the recovery process far smoother and less disruptive.
>
> Without documented procedures for bringing systems back online and with the employee who had originally configured the servers no longer with the agency, there was a significant loss of institutional knowledge. The agency was forced to rely on the vendor that sold them the servers to assist in safely restoring operations—a harrowing, time-consuming process that severely impacted their ability to serve customers. While they ultimately succeeded, this situation underscores the critical need for documented incident response, disaster recovery, and business continuity plans to ensure smoother, more efficient recovery in the event of a crisis. [178]

As seen in Figure 33, of the entire group of agencies surveyed, 57% do not have a documented cybersecurity incident response plan. If these agencies experience a hack, they will be forced to scramble, making it much more likely they make errors that make system recovery, customer notification, and operational continuity more difficult. The authors interviewed a representative from a mid-sized agency that did not have a document cybersecurity incident response plan in place when it was hacked and the consequences were significant.

One caveat to the concerning lack of adoption of cybersecurity response plans is that some agencies may have cybersecurity incident response planning built into their disaster response plan. Because of this possibility, a generous approach might be to include all agencies with either a disaster response plan, a cybersecurity response plan, or both.

[178] Author Interview, August 5, 2024.

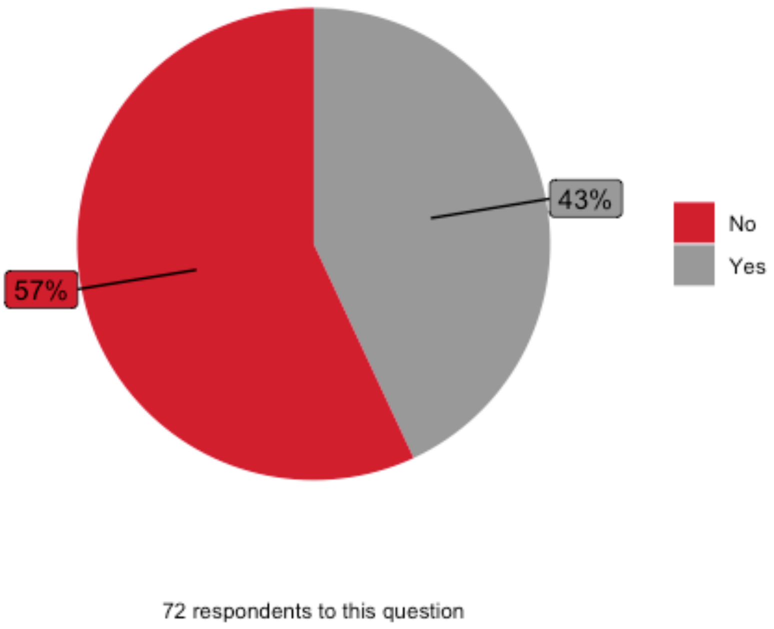


Figure 33. Cybersecurity Incident Response Plan Adoption

CISA recommends that organizations review their cybersecurity incident response plans quarterly and NIST recommends updating them annually. Twenty percent of the agencies with a cybersecurity incident response plan reported not updating it in the last year.

For this best practice, the largest agencies, those with budgets above $50M, showed significant adoption, while agencies having budgets below $50M dropped off significantly.

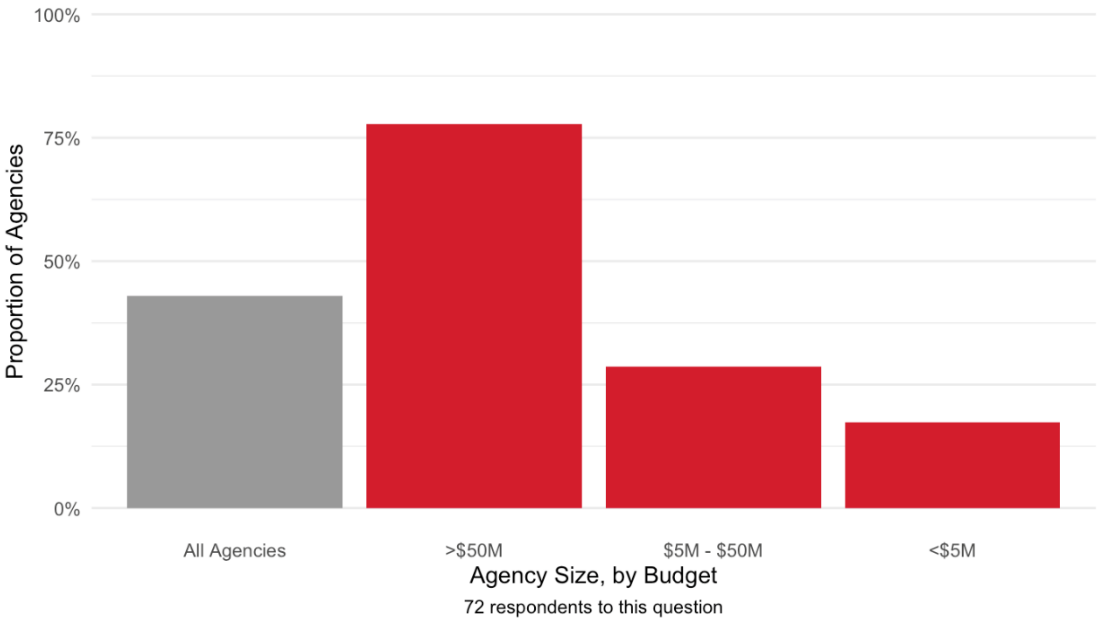


Figure 34. Proportion of Agencies with a Documented Cybersecurity Incident Response Plan

5.7 Tabletop Exercises

A disaster response plan or cybersecurity incident response plan is most effective when it is regularly reviewed, updated, and practiced, to ensure it remains relevant and actionable. This practice, known as a tabletop exercise, involves simulating potential scenarios to test the plan's effectiveness and the organization's readiness to respond. Conducting these exercises at least annually is crucial to account for evolving best practices, organizational changes, employee turnover, and the need for continuous training. Regular tabletop exercises not only improve preparedness but also build confidence and coordination among team members when responding to real-world incidents. The previous survey did not explore this practice, so no comment on a change in practice over time has been made.

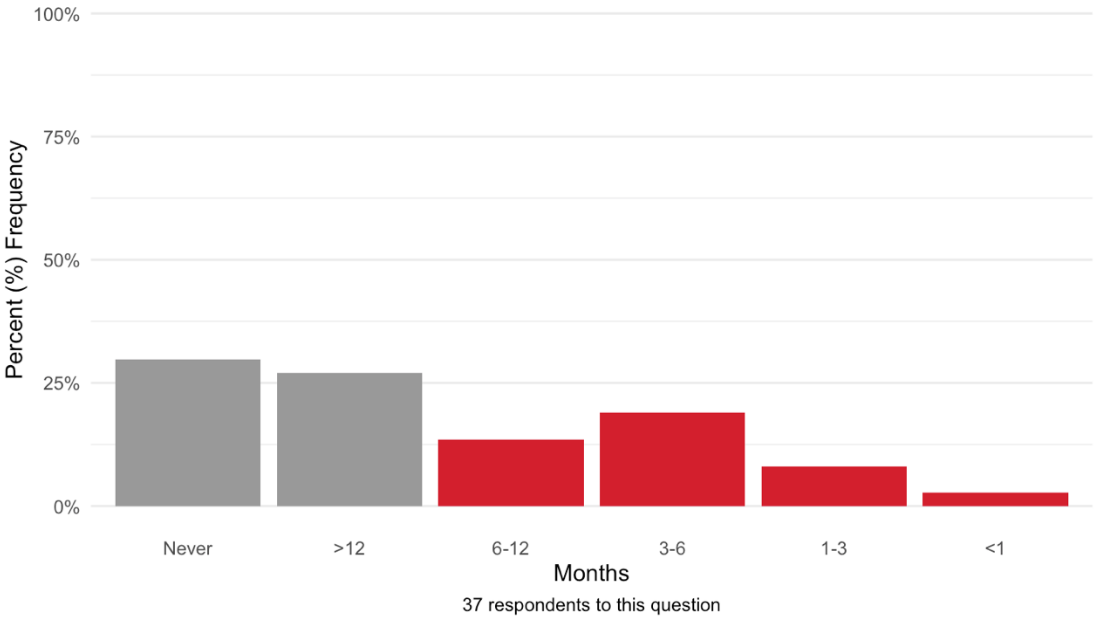


Figure 35. Time Since Last Tabletop Exercise

Of the agencies that reported having a disaster response plan, almost 60% did not conduct a tabletop exercise in the last year. This means that less than 40% of agencies had a disaster response plan that they practiced. Again, there was a significant drop off for those agencies that have budgets less than $50M.

Adoption of this practice showed the steepest drop-off of any of the factors analyzed in this survey. Only one agency with an operating budget of less than $50M reported conducting a tabletop exercise.

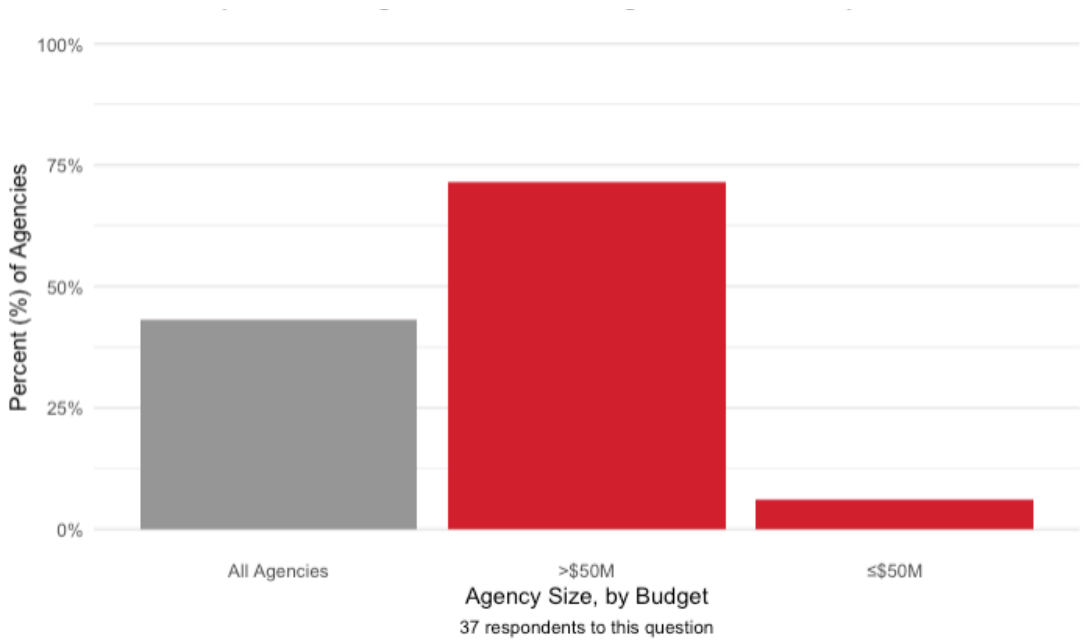


Figure 36. Proportion of Agencies Conducting Annual Tabletop Exercises

5.8 Log Retention Policies

Another important policy for agencies to establish is a log retention schedule. Logs provide a record of access to systems, database changes, server traffic, application updates, and other events across an organization's IT systems. In the event of a security threat, effective log retention can give agencies the information they need to pinpoint when the hack occurred, the threat presented, and the systems affected. This is especially true given that the average time from a security breach to its discovery is between 100 and 200 days.[180] To pinpoint a threat that has been present in a system for that long, system operators must rely on detailed logs. Because of this, many security standards, including PCI DSS, require critical logs to be retained for at least one year.[181]

The agencies that completed both surveys reported shorter log retention periods in 2024 than in 2020, as shown in Figure 37.

[180] Patrick Sites, "What Is Log Retention? Overview and Best Practices," LogicMonitor, September 18, 2024. https://www.logicmonitor.com/blog/what-is-log-retention.
[181] "Guidance on NIST 800-171 Log Retention," Consult DTS, accessed August 29, 2024, https://consultdts.com/article/nist-800-171-log-retention/.

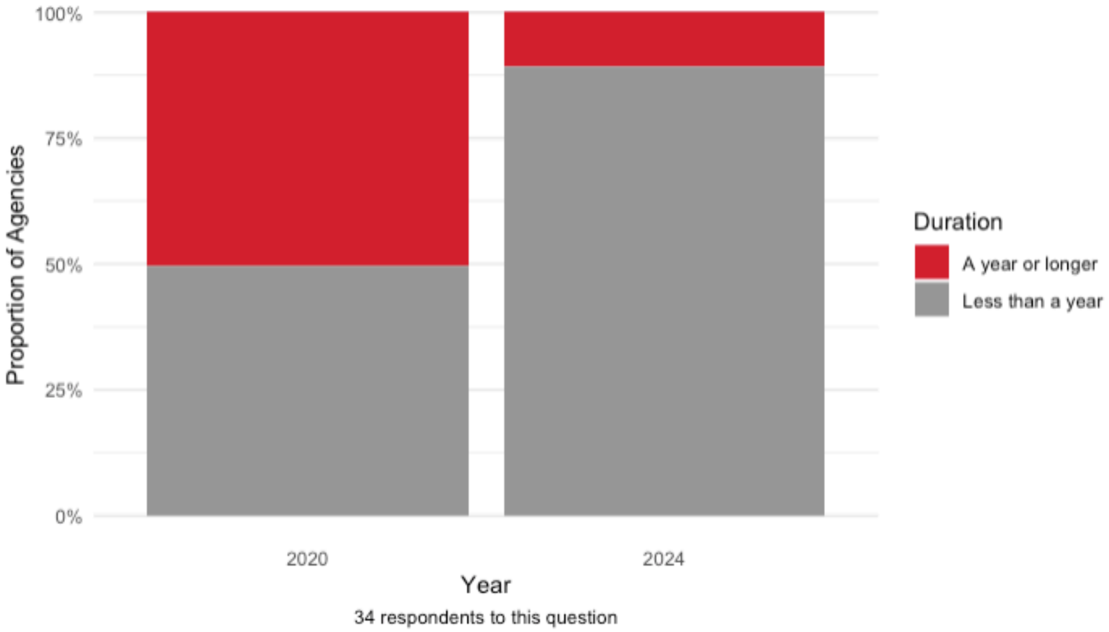


Figure 37. Log Retention Periods Over Time

Of agencies surveyed, over 70% of respondents reported not retaining any logs for longer than a year. While it is true that not all logs need to be retained for extended periods—since some data may lose relevance, not pose security risks, or lack justification for retention—it is equally important to recognize that certain types of logs should be retained beyond a year to support compliance, forensics, and operational analysis.

Best practice adoption worsened as size decreased, though adoption was low across all agencies, as seen in Figure 38.

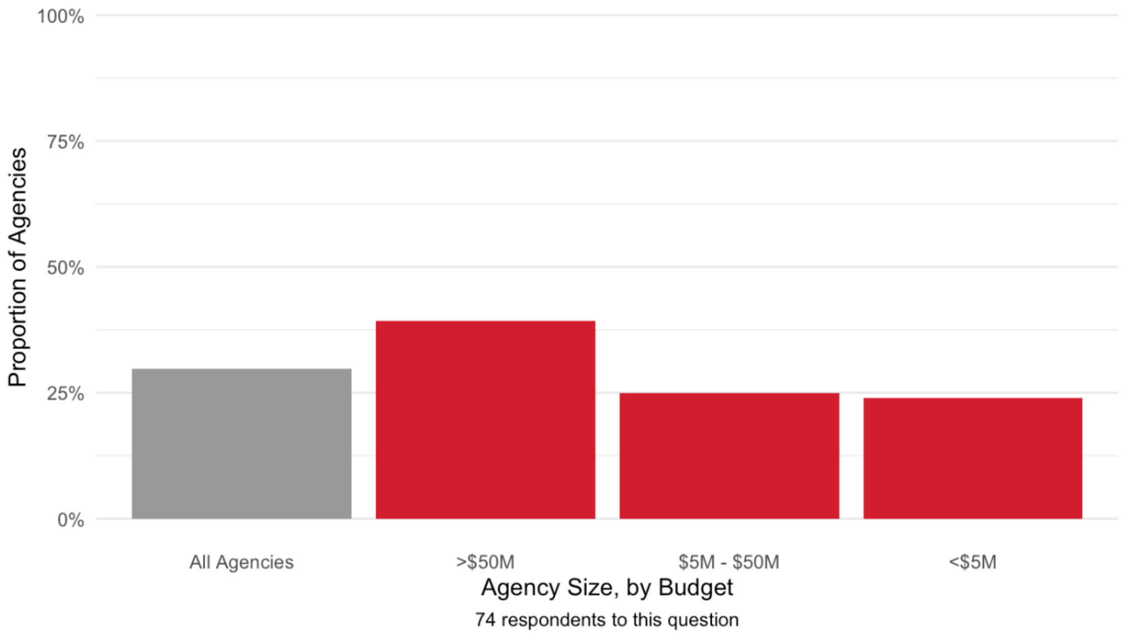


Figure 38. Proportion of Agencies Retaining Logs for a Year or More

Taken together, this data reveals serious concerns about the industry's preparation for, and ability to respond to, a cybersecurity incident when it occurs. For each question, a significant number of the respondents—if not the majority—are not following industry best practice. These policies and procedures are basic practices that organizations of all types of can—and should—have. Most agencies can avail themselves of free resources provided by organizations such as CISA or NIST to achieve compliance with best practice. For the five measures discussed above, best practices would involve:

- Having a documented cybersecurity policy that is updated at least annually.
- Having a documented disaster response plan that is updated at least annually.
- Having a documented cybersecurity incident response plan that is updated at least annually.
- Conducting tabletop exercises at least annually.
- Having a document log retention schedule and maintaining critical logs for at least one year.

Of the 78 agencies that responded to the survey, only five achieved these five best practices, and all of these agencies had operating budgets over $100 million. Moreover, the authors did not survey other critical practices, such as password management, multi-factor authentication, and differentiated access control, under the incorrect assumption that these were best practices already widely implemented across the industry. This oversight highlights the need to validate the actual adoption of foundational cybersecurity measures, rather than assuming their prevalence, as gaps in these basic practices can significantly undermine overall security.

Finding 3: Small Agencies are Lagging far Behind Large Ones

In the previous two sections, size-related disparities in best practice adherence were identified for the reader. For all the best practices cited, a higher proportion of larger agencies adhered than did the smaller agencies.

The best practices as laid out in Findings 1 and 2 are:

- Conduct a Cybersecurity Assessment at least annually
- Employ at least one person with a Cybersecurity Certification
- Conduct Cybersecurity Training at least annually
- Maintain an annually updated, documented Cybersecurity Policy
- Maintain an annually updated, documented Disaster Response Plan
- Maintain an annually updated, documented Cybersecurity Incident Response Plan
- Conduct annual Tabletop Exercises
- Retain critical System Logs for at least a year

In this finding, overall trends related to agency size in adherence to these best practices will be explained. To that end, each agency was given a percentage score which corresponded to the portion of the above best practices the agency followed.[182] Figure 39 is a graph of the average scores by agency size.

[182] Non-responses were not counted, so an agency that followed three best practices and did not respond to a question about one best practice would receive a score of 3/7, or approximately 43%.

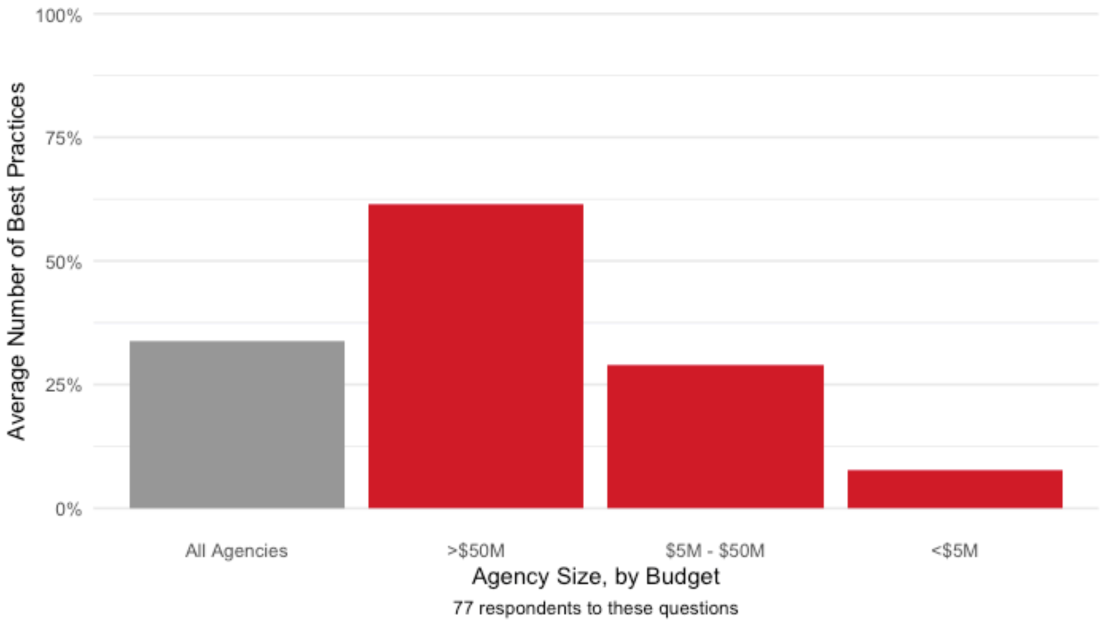


Figure 39. Average Proportion of Best Practices Followed by Size

The good news is that agencies with budgets above $50M are implementing approximately 60% of best practices. This level of implementation equates to twice as many best practices as those agencies with budgets between $5M and $50M, which are implementing roughly two best practices. The smallest category, agencies with budgets below $5M, are implementing less.

The practices scored in Figure 39 are the same standards applied earlier in the findings section, representing established best practices created or endorsed across a wide range of government and industry entities. Failing to meet one of these best practices, however, may not reflect the fact that an agency is not working towards doing so. For example, an agency with a cybersecurity policy that was last updated three years ago would fail to meet best practice standard; best practice requires annual updates to this policy. However, having a slightly out of date policy is better than having no policy at all. To reflect this nuance, the authors also graded the agencies against a less stringent set of standards. For these more basic standards, the authors eliminated the frequency requirements, meaning that credit was given for having a policy or conducting a practice, even if it was not updated or conducted as often as best practice advises. These more basic standards should provide insights into which practices agencies are working towards.

Under a more generous approach, the outlook improves. The pattern of decreasing adherence as size decreases is still reflected, but the data shows that even the smallest category of agencies is putting forth effort on some best practices.

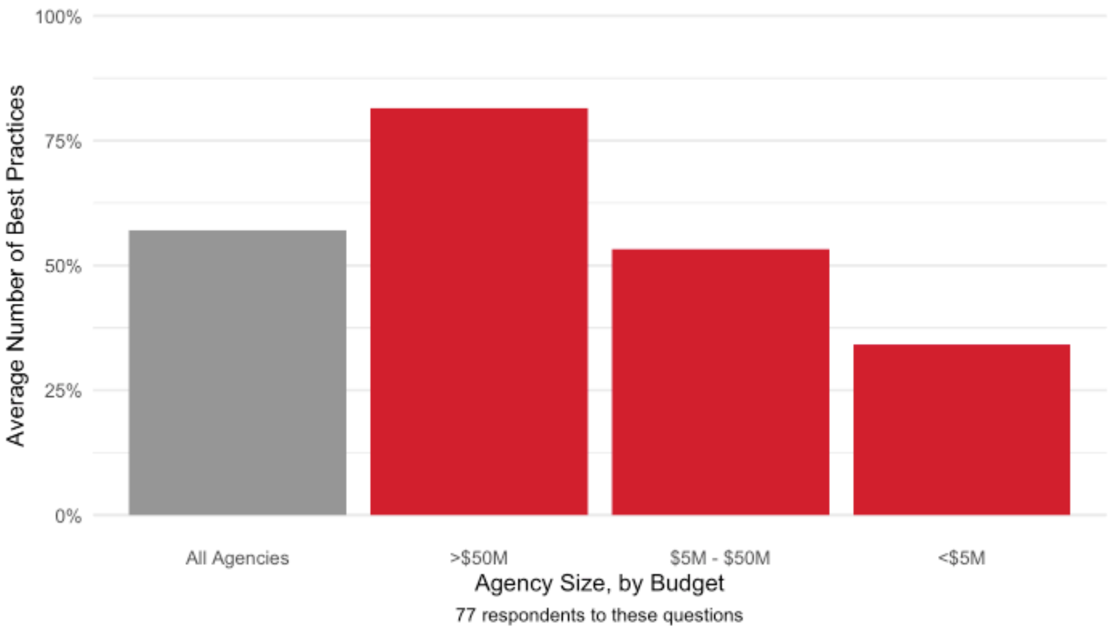


Figure 40. Average Best Practice Scores by Size

In Figure 40, the score distribution for these more generous standards is shown, and a pattern emerges. For the largest category of agencies, most agencies demonstrate progress towards almost all of the best practices, while smaller agencies are showing progress towards a lesser number of best practices.

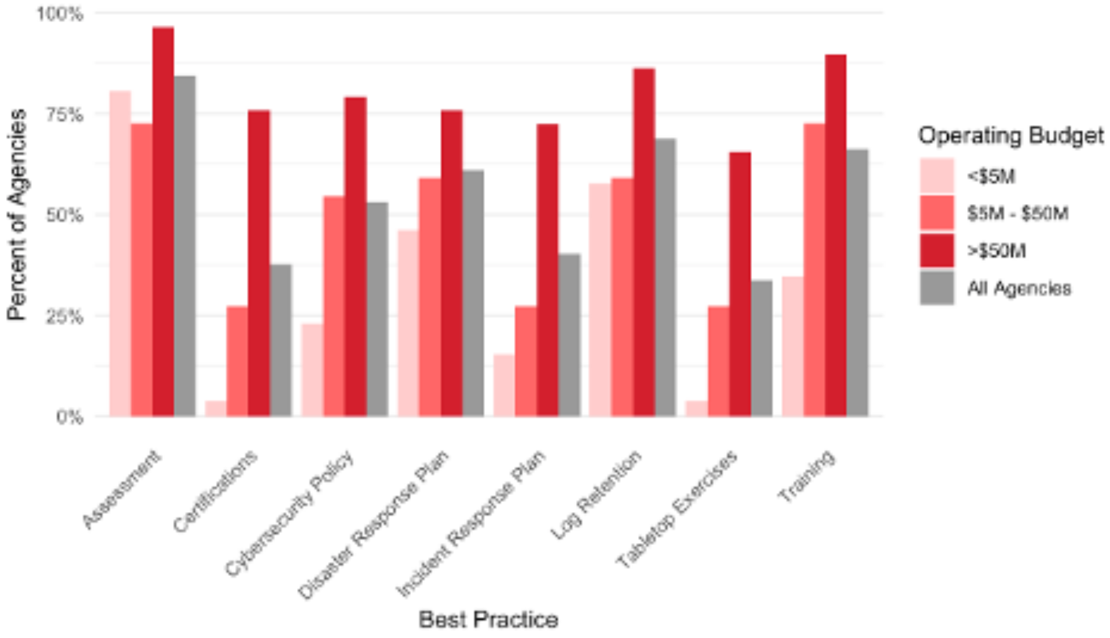


Figure 41. Basic Standards Adherence by Operating Budget

Cybersecurity assessment was the practice best adhered to across all respondents, followed by training. When agencies are judged against more generous standards, the results are more promising. Seventy-five or more percent of agencies in the largest category show progress towards, or attainment of, best practices for six of the eight best practices. For five of the eight practices, attainment of basic standards is above 50% for the entire group of respondents. While the smallest agencies continue to lag, they are meeting some basic practices.

6. Conclusion

The cybersecurity threat to public transit operations is real, yet many agencies continue to ignore the threat. They are not conducting regular cybersecurity assessments or putting basic policies and procedures in place to minimize the likelihood of a cybersecurity breach and to recover from the harm when one occurs. This observation was highlighted in the *2020 MTI Study* and has since been actively written about and discussed. While progress has been made by larger agencies since the *2020 MTI Study*, this study demonstrates that smaller agencies have not heeded the warnings and remain unprepared to respond to a cybersecurity attack. This inaction leaves them vulnerable to threats that could significantly disrupt operations, compromise data, and erode public trust.

Mitigating this threat and reducing its impact requires a concerted, coordinated effort among policy makers, transit agency leadership, industry representatives, and supporting organizations. Many small and mid-sized agencies simply do not have the resources to implement the best practices set forth above. When the 2024 findings were shared with Scott Bogren, the Executive Director of the Community Transportation Association of America (CTAA), he observed that the findings likely overstated small and rural agencies' actions to address cybersecurity, stating that "they simply do not have the financial or technical resources to take this on and without additional support cannot do so."[183]

Without a legislative mandate and resources, very little will change. To ensure that change occurs, Congress must act to require a basic cybersecurity program of all its federal aid recipients, provide the resources necessary to implement such a program, and use its oversight function to ensure that this happens in a timely manner. The executive branch must promulgate regulations implementing this mandate and make funding contingent on recipients having such programs in place. Transit agencies must avail themselves of the resources already at hand and those that will be made available if these recommendations are implemented. Finally, supporting organizations must continue to publicize, educate, train, and create tools for transit agencies to help them meet their cybersecurity needs. It is only with a focused, concerted effort by the entire ecosystem that transit agencies will make meaningful progress.

[183] Author interview, August 2, 2024.

7. Policy Recommendations

In response to the findings described in the previous section, the authors propose the following policy recommendations.

7.1 Congress

- Congress should provide funding to the DHS and the U.S. DOT, and the Co-Sector Risk Management Agencies for the Transportation Systems Sector (TSS) to develop and promulgate a set of minimal cybersecurity standards, programs to support agencies in coming into compliance with the minimal cybersecurity standards, and tools and for their promotion.

- Congress should increase formula grant funding to transit agencies to ensure that they have sufficient resources to meet the minimal cybersecurity standards established above and establish a minimum percentage of such funds that must be spent on cybersecurity.

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

- Congress should provide the DHS and the U.S. DOT the resources necessary to provide technical guidance to transit agencies in implementing the cybersecurity standards and practices established above.

- Through its oversight powers, Congress should ensure that the DHS and the U.S. DOT promulgate a regulation establishing a minimal set of cybersecurity requirements in a timely manner, continue to enhance and update this minimal set of standards, and establish the technical assistance and promotional programs necessary and practices established above and enforce their implementation.

7.2 Executive Branch

- The DHS and the U.S. DOT, working with input from industry associations and other supporting organizations (collectively, Supporting Organizations), should promulgate a set of minimum cybersecurity standards and practices that transit agencies must implement to receive formula and discretionary grant funding.

- The DHS should minimally require that all transit agencies meet the basic requirements set forth in TSA Information Circular IC-2021-01, "Enhancing Surface Transportation Cybersecurity TSA Circular for Surface Transportation."

- The DHS and the U.S. DOT should provide technical guidance to transit agencies to meet the new requirements set forth above.

- The U.S. DOT, working with the DHS, should create an attestation program, whereby transit CEOs and state Departments of Transportation executives are required to attest that their organization has met the minimum cybersecurity standards established above prior to receiving federal funds.

- The U.S. DOT and the DHS should continue to update and strengthen the minimal cybersecurity requirements being adopted as well as the technical assistance and promotional programs necessary to ensure that transit agencies are aware of their evolution and have the resources necessary to implement the changes.

7.3 Transit Agencies

- Transit Agencies should develop an individualized cybersecurity plan that takes advantage of the best practices identified above and update it at least annually.

- Transit Agencies should regularly brief their Board on the organization's cybersecurity assessment plan to address and prioritize risks and review progress.

- Transit Agencies should conduct a cybersecurity assessment at least annually and address the shortcomings identified in that assessment in a timely manner.

- Transit Agencies should ensure that they have documented cybersecurity policies and procedures in place and that the organization is following them.

- Transit Agencies should develop a disaster response plan, review it quarterly, update it annually, and train employees on it regularly to ensure preparedness.

- Transit Agencies should develop a cybersecurity incident response plan, review it quarterly, update it annually, and train employees on it regularly to ensure preparedness.

- Transit Agencies should conduct an audit of all external contracts and ensure that all software and hardware contracts have current and robust cybersecurity contract language in them protecting the Transit Operator and if not, act to remedy.

- Transit Agencies should ensure all new vendor contracts include standard cybersecurity contract language, allocating risk, and ensuring that vendors follow cybersecurity best practices.

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

- Transit Agencies should ensure that they have at least one person on staff with a cybersecurity certificate and are qualified to oversee the overall cybersecurity program and/or cybersecurity vendors.

- Transit Agencies should ensure that they have adequate cybersecurity insurance and if self-insuring, adequate reserves to cover any losses.

Associations and Other Supporting Organizations

- Industry Associations and other supporting organizations (collectively, Supporting Organizations) should develop a common clearinghouse for transit cybersecurity best practices.

- Supporting Organizations should create minimum guidelines for cybersecurity assessments and encourage cross-agency collaboration.

- Supporting Organizations should develop model cybersecurity contract language for agencies to integrate into their vendor contracts.

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

- Supporting Organizations should continue to develop cybersecurity training modules and certificates. In doing so they are able to take advantage of the guidance developed by TSS, CSAs, and others.

Appendix A – MTI Digital Survey Questions

Cybersecurity Benchmarking Study (2024)

1. Organization name
2. Your name
3. Your job title
4. Your phone number
5. What was your organization's annual budget in the most recent fiscal year?
6. How many full-time equivalents (FTEs) do you employ?
7. What is your annual budget for IT?
8. What is your current IT headcount? (FTEs)
9. What is your annual budget for cybersecurity?
10. What is your current cybersecurity headcount? (FTEs)
11. What modes of transit does your organization provide?
12. Who is charge of cybersecurity in your organization?
13. Do you receive direction, requirements, or process guidance from a local government CISO?
14. Have you engaged outside vendors to provide tools, software or support to assist with cybersecurity preparedness?
15. Have you engaged outside vendors to provide tools, software or support to assist with cyber response?
16. Do you or one of your staff have one or more cybersecurity related certifications? If yes, what are they? (Select all certifications earned by at least one staff member or yourself)
17. Do you have an individual that is responsible for cybersecurity response seven days a week and 24 hours a day?

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

19. Do you have the resources (e.g., funding, training, other support, and insurance coverage) you believe you need for cyber response?

20. Do you have access to the necessary information and guidance that you need to implement your cybersecurity preparedness program?

21. How prepared would you say your organization is in defending against cybersecurity threats?

22. How prepared would you say your organization is in responding to cybersecurity threats?

23. How often do you perform cybersecurity assessments?

24. When was the last time you conducted a cybersecurity assessment?

25. What tool do you use to conduct your assessments?

26. Do you self-assess or use external support?

27. Do you have a documented cybersecurity policy?

28. How often do you update your documented cybersecurity policy?

29. When was the last time you revised your documented cybersecurity policy?

30. Do you have a documented disaster response plan?

31. How often do you update your documented disaster response plan?

32. When was the last time you revised your documented disaster response plan?

33. When was your last tabletop exercise?

34. Do you have a documented cybersecurity incident response plan?

35. How often do you update your documented cybersecurity incident response plan?

36. When was the last time you revised your documented cybersecurity incident response plan?

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

38. Is the cybersecurity preparedness audit program internal or external?

39. How frequent is the cybersecurity preparedness audit?

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

41. Do you have a documented log maintenance schedule? If so, how long do you retain logs? Answer based on the type of logs you keep for the longest amount of time.

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

43. Do you conduct cybersecurity training? If so, how often?

44. Is the cybersecurity training different for different types of employees?

45. Have you had an incident? An incident is described as a cybersecurity event where an intrusion was made into your systems, and a material loss or disruption occurred. A material loss is considered in the form of data (>1,000 data records lost) or monies (>$10,000). A disruption is material if operations systems were offline for greater than 1 hour.

46. How many incidents have you had in the last year? An incident is described as a cybersecurity event where an intrusion was made into your systems, and a material loss or disruption occurred. A material loss is considered in the form of data (>1,000 data records lost) or monies (>$10,000). A disruption is material if operations systems were offline for greater than 1 hour.

47. To whom did you report the most recent incident?

48. Do you have cyber insurance?

49. What is your total annual cyber insurance coverage limit?

50. How has your cyber insurance annual coverage limit changed compared to three years ago?

51. What is the annual cost of your cyber insurance policy?

52. How has your cyber insurance annual cost changed compared to three years ago?

53. How has the coverage (e.g., types of events covered) of your cyber insurance policy change over the past three years?

54. Do you participate in an insurance pool?

Bibliography

American Association of State Highway Transportation Officials (AASHTO). "Council on Public Transportation." Accessed May 15, 2024. https://transportation.org/ptc/research/.

American Journal of Transportation. "How Cyber Attacks Are Impacting Transportation Systems." August 22, 2024. https://www.ajot.com/news/how-cyber-attacks-are-impacting-transportation-systems.

American Public Transportation Association (APTA). "Cybersecurity Fundamentals for Senior Executives." (video). November 7, 2024. https://learning.aptagateway.com/products/cybersecurity-fundamentals-for-executives.

American Public Transportation Association (APTA). "Cybersecurity Resources." Accessed, July 8, 2024. https://www.apta.com/research-technical-resources/safety-security/cybersecurity-resources/.

American Public Transportation Association (APTA). "Mobility Innovation Hub." Accessed October 9, 2024. https://www.apta.com/research-technical-resources/mobility-innovation-hub/.

Andrews, Garrett,. "Cybersecurity Salary Guide: How Much Can You Earn?" *Forbes*. February 20, 2024, https://www.forbes.com/advisor/education/it-and-tech/cybersecurity-salary-outlook/.

Australian Government, and the Australian Signals Directorate's Australian Cyber Security Center (ASD's ACSC). *Best Practices for Event Logging and Threat Detection*. Accessed September 8, 2024. https://www.cyber.gov.au/sites/default/files/2024-08/best-practices-for-event-logging-and-threat-detection.pdf.

BakerHostetler, *Data Security Incident Response Report*. April 23, 2024. https://admin.bakerlaw.com/wp-content/uploads/2024/04/2024-DSIR-Report-Web.pdf.

Belcher, Scott, Terri Belcher, Eric Greenwald, and 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.

Belcher, Scott, Terri Belcher, Kathryn Seekman, Brandon Thomas, Homayun Yaqub. "Aligning the Transit Industry and Their Vendors in the Face of Increasing Cyber Risk: Recommendations for Identifying and Addressing Cybersecurity Challenges." Mineta Transportation Institute, July 2022. DOI:10.31979/mti.2022.2113.

Belcher, Scott, and Todd Chollet. "Is There a Light at the End of the Tunnel? The Outlook for Cybersecurity Insurance and Transit in 2024." Mineta Transportation Institute, April 2024. https://transweb.sjsu.edu/press/There-Light-End-Tunnel-Outlook-Cybersecurity-Insurance-and-Transit-2024.

Bonina, Jared, and Matthew Dickens. *APTA Public Transportation Ridership Update*. APTA, April 2024. https://www.apta.com/wp-content/uploads/APTA-POLICY-BRIEF-Transit-Ridership-04.01.2024.pdf.

Burbidge, Timo. "Ransomware Threat Rises: Verizon 2022 Data Breach Investigations Report." Verizon, May 24, 2022, https://www.verizon.com/about/news/ransomware-threat-rises-verizon-2022-data-breach-investigations-report.

Bureau of Labor Statistics. "Employer Costs for Employee Compensation." September 10, 2024. https://www.bls.gov/news.release/pdf/ecec.pdf.

Bush, Bill. "Hackers Release Reams of Stolen Columbus Data on Dark Web." *The Columbus Dispatch*. August 8, 2024. https://www.dispatch.com/story/news/local/2024/08/08/city-columbus-data-public-dark-web-ransomware-hack-cyber-ohio-cybersecurity-stolen/74718671007/.

BYD. "Buy America." Accessed October 10, 2024. https://en.byd.com/news/buy-america/#:~:text=All%20our%20bus%20models%20in,American%20vendors%20across%20the%20nation.

Chandler, Kevin L., Jodi M. Rizek, and Pamela J. Sutherland. *Security and Emergency Preparedness Action Items for Transit Agencies*. Federal Transit Administration (FTA), September 2014. https://www.transit.dot.gov/sites/fta.dot.gov/files/docs/508_new_top_17.pdf.

Chew, Tan Soon. "Considerations for Developing Cybersecurity Awareness Training." ISACA, March 1, 2023. https://www.isaca.org/resources/isaca-journal/issues/2023/volume-2/considerations-for-developing-cybersecurity-awareness-training#:~:text=Frequency%20of%20Training,forget%20what%20they%20have%20learned.

Code of Federal Regulation. 49 CFR. "Transportation." §661

Code of Federal Regulations. 49 CFR. "Transportation." §663.13.

Community Transportation Association of America (CTAA). *Strategic Plan 2021–2025*. Accessed September 15, 2024. https://ctaa.org/wp-content/uploads/2021/09/CTAA-Strategic-Plan-FInal-1.pdf.

Contestabile, John, Paul Lennon, Christopher Lyons, and Rick Tiene. "Issue Brief: Cybersecurity; Is Cybersecurity a Core Safety Issue for Transportation?" Intelligent Transportation Society of America (ITS, America), July 2024. https://itsa.org/wp-content/uploads/2024/07/Cybersecurity-and-Transportation-Safety-Issue-Brief-Final-Version.pdf.

Cybersecurity & Infrastructure Security Agency (CISA). "About CISA." Accessed August 29, 2024. https://www.cisa.gov/about-cisa.

Cybersecurity & Infrastructure Security Agency (CISA). "Avoiding Social Engineering and Phishing Attacks." February 1, 2021. https://www.cisa.gov/news-events/news/avoiding-social-engineering-and-phishing-attacks.

Cybersecurity & Infrastructure Security Agency (CISA). "Critical Infrastructure Sectors." Accessed August 29, 2024. https://www.dhs.gov/cisa/critical-infrastructure-sectors.

Cybersecurity & Infrastructure Security Agency (CISA). "Cross-Sector Cybersecurity Performance Goals." Accessed September 20, 2024. https://www.cisa.gov/sites/default/files/publications/2022_00092_CISA_CPG_Report_508c.pdf.

Cybersecurity & Infrastructure Security Agency (CISA). "Cyber-Hygiene Services." Accessed August 29, 2024. https://www.cisa.gov/cyber-hygiene-services.

Cybersecurity & Infrastructure Security Agency (CISA). "Cybersecurity Advisory Committee." Accessed August 13, 2024. https://www.cisa.gov/resources-tools/groups/cisa-cybersecurity-advisory-committee ()

Cybersecurity & Infrastructure Agency (CISA). "Cybersecurity Best Practices." Accessed October 22, 2024. https://www.cisa.gov/topics/cybersecurity-best-practices

Cybersecurity & Infrastructure Security Agency. "Incident Response Plan (IRP) Basics." Accessed October 10, 2024. https://www.cisa.gov/sites/default/files/publications/Incident-Response-Plan-Basics_508c.pdf.

Cybersecurity & Infrastructure Security Agency (CISA). “Infrastructure Resilience Planning Framework (IRPF).” Version 1.2. February 2024. Accessed July 23, 2024. https://www.cisa.gov/sites/default/files/2024-03/infrastructure-resilience-planning-framework03-22-2024.pdf.

Cybersecurity & Infrastructure Security Agency (CISA). “Infrastructure Resilience Planning Framework Playbook.” June 2024. Accessed September 20, 2024. https://www.cisa.gov/resources-tools/resources/infrastructure-resilience-planning-framework-irpf-playbook

Cybersecurity & Infrastructure Security Agency (CISA). “Require Strong Passwords.” Accessed August 29, 2024. https://www.cisa.gov/secure-our-world/require-strong-passwords#:~:text=Require%20strong%2C%20unique%20passwords.,of%205%20%E2%80%937%20random%20words.

“Cybersecurity” U.S.DOT Intelligent Transportation Systems, Joint Program Office, access date March 18, 2025https://www.its.dot.gov/resources/Cybersecurity/

Dell Technologies. “Global Data Protection Index Survey – Special Edition 2024.” October 2023. Accessed August 29, 2024. https://www.dell.com/en-us/lp/dt/data-protection-gdpi.

Department of Homeland Security. “Enhancing Public Transportation and Passenger Railroad Cybersecurity.” Security Directive 1582-21-01C. Transportation Security Administration (TSA), effective October 24, 2024. https://www.tsa.gov/sites/default/files/security_directive_1582-21-01c_and_memo_508c.pdf.

Department of Homeland Security. “Enhancing Public Transportation and Passenger Railroad Cybersecurity.” Security Directive 1582-21-01B. Transportation Security Administration (TSA), effective October 24, 2023. https://www.tsa.gov/sites/default/files/sd-1582-21-01b-enhancing-public-transportation-and-passenger-railroad-cybersecurity.pdf.

Department of Homeland Security. “Enhancing Surface Transportation Cybersecurity.” Surface Transportation IC-2021-01, effective December 31, 2021. Transportation Security Agency (TSA). https://www.tsa.gov/sites/default/files/20211201_surface-ic-2021-01.pdf.

Department of Homeland Security (DHS), Transportation Security Administration. “Security Training for Surface Transportation Employees; Extension of Compliance Dates; Correcting Amendments.” *86 FR 23629*. effective May 4, 2021. https://www.federalregister.gov/documents/2021/05/04/2021-09394/security-training-for-surface-transportation-employees-extension-of-compliance-dates-correcting.

Department of Homeland Security (DHS). *Cybersecurity Advisors*. 2017. https://www.bu.edu/tech/files/2017/09/DHS_CSA_Fact_Sheet_2017-1.pdf.

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.

Department of Justice. "Leader of Massive Scheme to Traffic in Fraudulent and Counterfeit Cisco Networking Equipment Sentenced to Prison." May 2, 2024. https://www.justice.gov/opa/pr/leader-massive-scheme-traffic-fraudulent-and-counterfeit-cisco-networking-equipment.

Department of Transportation. "Cybersecurity Discretionary Grant Projects." Accessed September 22, 2024. https://www.transportation.gov/CIO/cybersecurity-discretionary-grant-projects.

Department of Transportation (DOT). "SMART Grants Notice of Funding Opportunity." August 25, 2023. https://www.transportation.gov/sites/dot.gov/files/2023-08/Final%20SMART%20FY23%20Stage%201%20NOFO_0.pdf.

Department of Transportation (DOT). "How the U.S. Department of Transportation is Protecting the Connected Transportation Systems from Cyber Threats." accessed October 13, 2024. https://www.its.dot.gov/factsheets/pdf/cybersecurity_factsheet.pdf.

Department of Transportation (DOT), "National Cybersecurity Strategy." March 2023. https://www.whitehouse.gov/wp-content/uploads/2023/03/National-Cybersecurity-Strategy-2023.pdf.

Department of Transportation, (DOT). "Office of the Chief Information Officer." Accessed September 22, 2024. https://www.transportation.gov/cio.

Department of Transportation (DOT). "Office of Sector Cyber Coordination." Accessed September 22, 2024. https://www.transportation.gov/mission/office-secretary/office-chief-information-officer/office-sector-cyber-coordination.

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

Dickens, Matthew, and David Kahana. *Public Transportation Fare Database*. American Public Transportation Association (APTA), 2022. https://www.apta.com/research-technical-resources/transit-statistics/fare-database/.

Dickens, Matthew. *2023 Public Transportation Fact Book*. 74th ed. APTA, March 2024. https://www.apta.com/wp-content/uploads/APTA-2023-Public-Transportation-Fact-Book.pdf

DTS. "Guidance on NIST 800-171 Log Retention." January 22, 2024. https://consultdts.com/article/nist-800-171-log-retention/.

Edison Electric Institute. *Model Procurement Contract Language Addressing Cybersecurity Supply Chain Risk*. October 2022. https://www.eei.org/-/media/Project/EEI/Documents/Issues-and-Policy/Model--Procurement-Contract.pdf.

Enterprise Cyber Security Working Group. *Cybersecurity Considerations for Public Transit*. APTA, 2022. https://www.apta.com/wp-content/uploads/APTA-SS-ECS-RP-001-14_R1.pdf.

Faulhaber, Joe, and Brad Moon. "Small Business Cyber Attack Analysis: Most Targeted SMB Sectors and Key Prevention Tips." CrowdStrike. January 30, 2023. https://www.crowdstrike.com/en-us/blog/small-business-cyberattack-analysis-most-targeted-smb-sectors/.

Federal Bureau of Investigation (FBI). *Internet Crime Report 2023*. March 6, 2024. https://www.ic3.gov/Media/PDF/AnnualReport/2023_IC3Report.pdf

Federal Bureau of Investigation (FBI). "Director Christopher Wray's Remarks at Press Conference Announcing the Disruption of the Hive Ransomware Group." January 26, 2023. https://www.fbi.gov/news/speeches/director-christopher-wrays-remarks-at-press-conference-announcing-the-disruption-of-the-hive-ransomware-group.

Federal Communication Commission (FCC). "Letter from Jessica Rosenworcel, Chairwoman of the Federal Communications Commission, to Maria Cantwell, Chair or the Senate Committee on Commerce, Science, and Transportation." May 2, 2024. https://docs.fcc.gov/public/attachments/DOC-402312A1.pdf.

Federal Transit Administration (FTA). *2022 Annual Database Agency Information*. Updated July 17, 2024. https://www.transit.dot.gov/ntd/data-product/2022-annual-database-agency-information.

Federal Transit Administration (FTA). "2022 Annual Database Operating Expenses." April 12, 2024. https://www.transit.dot.gov/ntd/data-product/2022-annual-database-operating-expenses.

Federal Transit Administration (FTA). *Contractor Manual, Fiscal Year 2024*. DOT (2024). https://www.transit.dot.gov/sites/fta.dot.gov/files/2024-03/Fiscal-Year-2024-Contractor-Manual_0.pdf.

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

Federal Transit Administration (FTA). "Cybersecurity Resources for Transit Agencies." Accessed September 22, 2024. https://www.transit.dot.gov/regulations-and-programs/safety/cybersecurity-resources-transit-agencies#:~:text=Cybersecurity%20is%20now%20a%20component,both%20physical%20and%20cyber%20threats.

Federal Transit Administration (FTA). "Formula Grants for Rural Areas." accessed August 2, 2024. https://www.transit.dot.gov/funding/grants/urbanized-area-formula-grants-5307.

Federal Transit Administration (FTA). "Raw Monthly Ridership (No Adjustments or Estimates)." May 2024. https://www.transit.dot.gov/ntd/data-product/monthly-module-raw-data-release.

Federal Transit Administration (FTA). "The National Transit Database (NTD)." Last Updated May 14, 2024. Accessed October 14, 2024. https://www.transit.dot.gov/ntd.

Federal Transit Administration (FTA), Office of Research, Innovation and Demonstration, https://www.transit.dot.gov/regulations-and-programs/safety/cybersecurity-resources-transit-agencies (Accessed July,8, 2024)

Federal Transit Administration (FTA), 2022 Operating Expenses, https://www.transit.dot.gov/ntd/data-product/2022-operating-expenses (accessed August 6, 2024)

Federal Transit Administration (FTA). "Urban Area Formula Grant Program – 5311." Accessed August 2, 2024. https://www.transit.dot.gov/rural-formula-grants-5311.

Feuerborn, Mark. “Columbus Ransomware Attack: Rhysida Starts Data Leak before Changing Course.” NBC4i. Updated August 14, 2024. https://www.nbc4i.com/news/local-news/columbus/columbus-ransomware-attack-rhysida-announces-public-leak-before-changing-course/.

Forno, Richard. “What is Salt Typhoon? A Security Expert Explains the Chinese Hackers and Their Hacks on US Telecommunications Networks.” *UMBC Magazine*. December 6, 2024. https://umbc.edu/stories/what-is-salt-typhoon-a-security-expert-explains-the-chinese-hackers-and-their-attack-on-us-telecommunications-networks/.

Halcyon. “Ransomware Disrupts the Transit Authority of Northern Kentucky,” August 19, 2024. Accessed August 21, 2024. https://www.halcyon.ai/attacks/ransomware-attack-disrupts-northern-kentucky-transit-authority-tank.

Husain, Sohail, “Rural Transportation Challenges: Stakeholder Perspectives,” Eno Center for Transportation. March 22, 2024. https://enotrans.org/article/rural-transportation-challenges-stakeholder-perspectives/.

Hylender, C. David, Phillipe Langlios, Alex Pinto, and Suzanne Widup. *2024 Data Breach Investigations Report*. Verizon Business, May 1, 2024. https://www.verizon.com/business/resources/T348/reports/2024-dbir-data-breach-investigations-report.pdf.

IBM. *Cost of a Data Breach Report 2024*. July 30, 2024. https://www.ibm.com/search?lang=en&cc=us&q=cost%20of%20a%20data%20breach%20 2024.

Krause, Cory, and Justin Anderson, Kellen Shain, Linda Nana, Tom Mazzone, Stephen McNaught, and Mark Jackson. “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.

Lukasik, Dan, Jack Oden, Robert Sanchez, Brian Russell, Kyle Rush, and Adam Chandler. “Cybersecurity Language for Procurement of Intelligent Transportation Systems Equipment.” DOT. January 22, 2024. https://rosap.ntl.bts.gov/view/dot/73792.

National Academies of Science, Engineering, and Medicine. “About | Transportation Research Board.” Accessed September 15, 2024. https://www.nationalacademies.org/trb/about.

National Academies of Sciences, Engineering, and Medicine. *Cybersecurity in Transit Systems*. The National Academies Press, 2022. https://doi.org/10.17226/26475.

National Academies of Science, Engineering, and Medicine. *Developing a Physical and Cyber Security Primer for Transportation Agencies*. The National Academies Press, 2020. https://doi.org/10.17226/25869.

National Academies of Sciences, Engineering, and Medicine. *Cybersecurity Issues and Protection Strategies for State Transportation Agency CEOs: Volume 2, Transportation Cyber Risk Guide*. The National Academies Press, 2023. https://doi.org/10.17226/27035.

National Center for Applied Transit Technology. Accessed September 8, 2024. https://n-catt.org/.

"National Defense Authorization Act for Fiscal Year 2020, S.1760, 116th Congress (2021). https://www.congress.gov/bill/116th-congress/senate-bill/1790/text.

National Highway Traffic Safety Administration (NHTSA). Cybersecurity Best Practices for Modern Vehicles. DOT, updated 2022. https://www.nhtsa.gov/sites/nhtsa.gov/files/2022-09/cybersecurity-best-practices-safety-modern-vehicles-2022-tag.pdf.

National Highway Traffic Safety Administration (NHTSA). "Technology & Innovation." March 16, 2018. Accessed October 12, 2024. https://www.nhtsa.gov/technology-innovation.

National Institute of Standards and Technology (NIST). "*The NIST Cybersecurity Framework 2.0*." U.S. Department of Commerce, February 26, 2024. https://nvlpubs.nist.gov/nistpubs/CSWP/NIST.CSWP.29.pdf.

National Institute of Standards and Technology (NIST). "NIST Cybersecurity Framework 2.0: Quick Start Guide for Cybersecurity Supply Chain Risk Management (C-SCRM)." October 21, 2024. https://csrc.nist.gov/pubs/sp/1305/final.

National Institute of Standards and Technology (NIST). "NIST Cybersecurity Framework 2.0: Small Business Quick Start Guide." February 2024. https://csrc.nist.gov/pubs/sp/1300/final.

National Rural Transit Assistance Program. "National RTAP FAQs." Accessed September 8, 2024. https://www.nationalrtap.org/About/National-RTAP-FAQ.

NetDiligence Cyber Claims Study 2024 Report (Net Diligence, 2024), 9, https://netdiligence.com/wp-content/uploads/2024/09/NetDiligence-Cyber-Claims-Study-2024-Report-1.pdf.

Neuberger, Ann. “The Ransomware Battle is Changing – So Should Our Response.” *Financial Times*. October 3, 2024. https://www.ft.com/content/3b172a2a-4be5-4ef4-87cb-7fdcdee2ad99.

Noone, Dennis. “Transit Agency Faced Growing Problem, Chose Abnormal Solution.” Government Technology Industry Insider. March 13, 2023. https://insider.govtech.com/california/news/transit-agency-faced-growing-problem-chose-abnormal-solution.

North America Transit Cybersecurity Consortium, "Operational Technology Procurement Requirements," January 31, 2024, (accessed March 21, 2025) https://nacitcc.mta.info/NATCA_OT_Procurement_Requirements.pdf

“Notices.” Federal Register 89, no 175 (September 10, 2024): 73488–73489. https://www.govinfo.gov/content/pkg/FR-2024-09-10/pdf/2024-20331.pdf.

O’Neil, Lori Ross, Thomas E. Carroll, Entesar M. Abdelhadi, Mark D. Watson, Carol L. Hammer, and Maria B. Psarakris. *Sample Cybersecurity Clauses for EV Charging Infrastructure Procurements*. Joint Office of Energy and Transportation, 2023. https://www.pnnl.gov/main/publications/external/technical_reports/PNNL-34454.pdf.

Office of Budget and Policy. *2021 National Transit Database; National Transit Summaries & Trends*. Federal Transit Administration (FTA), November 2022. https://www.transit.dot.gov/sites/fta.dot.gov/files/2022-11/2021%20National%20Transit%20Summaries%20and%20Trends_1-1.pdf.

Office of Information Technology Services, *Federal Highway Administration (FHWA) Cybersecurity Program (CSP) Handbook*. FHWA. December 2017. https://www.fhwa.dot.gov/legsregs/directives/orders/csp_handbook.pdf.

Pattison-Gordon, Jule, and Noelle Knell. “How Two States Handle Cyber Security Risks from Vendors.” Government Technology. October 10 2014. https://www.govtech.com/security/how-two-states-handle-cybersecurity-risks-from-vendors?utm_campaign=Newsletter%20-%20GT%20-%20GovTech%20Today&utm_medium=email&_hsenc=p2ANqtz--DzlazjWlIKaNNTtQM3PPFAL_EHvV8zGIv978bYkp9Z3K3wZEWJHjYk4hlCFQe8SrnZCcYyWW-3VRWWtaURedMF82eJw&_hsmi=329834740&utm_content=329837483&utm_source=hs_email.

PCI Security Standards Council. “PCI Security.” Accessed July 9, 2024. https://east.pcisecuritystandards.org/pci_security/.

PCI Security Standards Council. "PCI SSC Work from Home: Security Awareness." Accessed August 29, 2024. https://blog.pcisecuritystandards.org/new-training-work-from-home-security-awareness.

Ribero, Anna. "FHWA Adopts Cybersecurity Evaluation Tool to Enhance Transportation Infrastructure Protection." Industrial Cyber. September 13, 2024. https://industrialcyber.co/transport/fhwa-adopts-cybersecurity-evaluation-tool-to-enhance-transportation-infrastructure-protection.

Richardson, Mahealani. "Rider Data Apparently Compromised in Alleged Ransomware Attach on TheBus, Handi-Van." Hawaii News Now. June 18, 2024. https://www.hawaiinewsnow.com/2024/06/19/ots-cyber-breach-allegedly-includes-800000-pieces-data/.

Roman, Alex. "Q&A with APTA Chair and JTA CEO Nathaniel P. Ford Sr." *METRO*. February 12, 2018. https://www.metro-magazine.com/10007328/qa-with-apta-chair-and-jta-ceo-nathaniel-p-ford-sr.

SentinelOne. "What is Credential Theft?" Accessed August 29, 2024. https://www.sentinelone.com/cybersecurity-101/what-is-credential-theft/.

Sites, Patrick. "What Is Log Retention? Overview and Best Practices." LogicMonitor. September 18, 2024. https://www.logicmonitor.com/blog/what-is-log-retention.

Snyder, Charles, and Rex Johnson. "Critical Infrastructure and the Rising Threats to Operational Technology." CAI. 2022. https://www.cai.io/resources/thought-leadership/critical-infrastructure-and-the-rising-threats-to-operational-technology#fn:4.

The White House. "FACT SHEET: Biden-Harris Administration Convenes Fourth Global Gathering to Counter Ransomware." October 2, 2024. https://bidenwhitehouse.archives.gov/briefing-room/statements-releases/2024/10/02/fact-sheet-biden-%E2%81%A0harris-administration-convenes-fourth-global-gathering-to-counter-ransomware/.

The White House. *National Cybersecurity Strategy Implementation Plan*. Version 2. May 2024. https://www.whitehouse.gov/wp-content/uploads/2024/05/NCSIP-Version-2-FINAL-May-2024.pdf.

The White House. *National Cybersecurity Strategy*. March 2023, https://www.whitehouse.gov/wp-content/uploads/2023/03/National-Cybersecurity-Strategy-2023.pdf.

Thrive DX. "Why Cyber Security Certifications Matter in Today's World." June 20, 2024. https://thrivedx.com/resources/blog/why-cybersecurity-certifications-matter-in-todays-world-2#:~:text=The%20Value%20of%20Cybersecurity%20Certifications,-Validation%20of%20Skills&text=Cybersecurity%20certifications%20are%20a%20benchmark,data%2C%20and%20prevent%20data%20breaches.

Transportation Security Administration (TSA). *TSA Cybersecurity Roadmap 2018*. November 2018. https://www.tsa.gov/sites/default/files/tsa_cybersecurity_roadmap.pdf.

Transportation Security Administration (TSA). "Mission." Accessed September 8, 2024. https://www.tsa.gov/about/tsa-mission.

Transportation Security Administration (TSA). *Security Resources for Mass Transit Systems*. Accessed August 21, 2024. https://www.tsa.gov/sites/default/files/tsa_mtpr_resources_slick_sheet.pdf.

Transportation Security Administration (TSA). "TSA Releases Cybersecurity Roadmap." December 4, 2018. Accessed August 18. 2024. https://www.tsa.gov/news/releases/2018/12/04/tsa-releases-cybersecurity-roadmap.

Volpe, John A. *The Public Transportation System Security and Emergency Preparedness Planning Guide*. FTA, January 2003. https://www.transit.dot.gov/sites/fta.dot.gov/files/docs/PlanningGuide.pdf.

Abbreviations and Acronyms

AASHTO	American Association of State Highway and Transportation Officials
ADA	Americans with Disabilities Act
APTA	American Public Transit Association
BART	Bay Area Rapid Transit
BASE	Baseline Assessment and Security Enhancement
BCP	Business Continuity Planning
BEC	Business Email Compromise
BRT	Bus-rapid transit
C-IST	Cyber Infrastructure Survey Tool
CATT	Cybersecurity Assessment Tool for Transit
CAD/AVL	Computer Aided Dispatch/Automatic Vehicle Location
CCSWG	Control Communications Security Working Group
CISA	Cybersecurity and Infrastructure Agency
CISO	Chief Information Security Officer
CPG	Cybersecurity Performance Goals
CRR	Cyber Resilience Review
CSA	Cybersecurity Advisors
CSET	Cyber Security Evaluation Tool
CTAA	Community Transportation Association of America
DR	Disaster Recovery
DSRC	Dedicated short range communications

ECSWG	Enterprise Cybersecurity Working Group
EDM	External Dependency Management
EDR	Endpoint Detection and Response
EO	Executive Order
FBI	Federal Bureau of Investigation
FCC	Federal Communications Commission
FEMA	Federal Emergency Management Agency
FHWA	Federal Highway Administration
FTA	Federal Transportation Agency
GPS	Global positioning systems
IMR	Incident Management Review
IR	Incident Response
IRPF	Infrastructure Resilience Planning Framework
ISAC	Information Sharing and Analysis Center
IST	Infrastructure Survey Tool
IT	Information Technology
ITSA	Intelligent Transportation Society of America
ITS JPO	Intelligent Transportation Systems Joint Program Office
MFA	Multi-Factor Authentication
MOD	Mobility on Demand
MTAP	Multi-State Transit Technical Assistance Program
MTI	Mineta Transportation Agency

N-CATT	National Center for Applied Transit Technology
NHTSA	National Highway Traffic Safety Administration
NIST	National Institute of Standards and Technology
NOFO	Notices of Funding Opportunity
NTD	National Transit Database
OEM	Original Equipment Manufacturers
OSTP	Office of Science and Technology Policy
OT	Operational Technology
OEM	Original Equipment Manufacturer
PCI	Payment Card Industry
PCI DSS	Payment Card Industry Data Security Standard
PCI SCC	Payment Card Industry Security Standards Council
PII	Personally Identifiable Information
PoLP	Principle of Least Privilege
PT-ISAC	Public Transportation Information Sharing and Analysis Center
RTAP	Rural Transit Assistance Program
SCADA	Supervisory Control and Data Acquisition
STSI	Surface Transportation Security Inspector
TNC	Transportation Network Companies
TRB	Transportation Research Board
TSA	Transportation Security Administration
TSS	Transportation Systems Sector

TTP	Tactics, Techniques, and Procedures
US DHS	United States Department of Homeland Security
US DOE	United States Department of Energy
US DOT	United States Department of Transportation
US-CERT	United States Computer Emergency Readiness Team
VPN	Virtual Private Network

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, the environment, and cybersecurity. Prior to founding 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 is a Mineta Transportation Institute (MTI) Research Associate and has a written a several white papers and two MTI studies on cybersecurity in transportation. Mr. Belcher has more than 35 years of private and public sector experience in Washington, D.C. Before ITS America, Mr. Belcher held senior management positions at a number of prominent trade associations, worked in private practice at the law firm Beveridge & Diamond PC, and worked at the U.S. Environmental Protection Agency. Mr. Belcher serves on a number of public and private advisory boards. He 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.

Terri Belcher

Terri Belcher is a writer and analyst who has worked in Washington, D.C. for the past 35 years. Ms. Belcher has 25 years of experience working for the federal government, federal contractors, and a number of non-profits. Ms. Belcher earned a Bachelor of Arts degree from the University of Redlands.

James Grimes

James Grimes was a research associate for SFB Consulting, LLC and Cybrbase from 2022–2024. Mr. Grimes has experience with data science and statistical analysis and completed several statistical research projects during his undergraduate studies at the University of Virginia (UVA). Mr. Grimes received his Bachelor of Arts from UVA in Economics and Statistics and graduated with Honors in 2024.

Lusa Holmstrom

Lusa Holmstrom is a dual degree student at Fordham University pursuing a Bachelor of Arts in English and Spanish and an MA in Education and will receive her undergraduate degree in May 2025. She is a writer and Assistant Opinion Editor at the *Fordham Ram* newspaper, works as a Maintenance Coordinator at Fordham University's Department of Transportation, and has three years of experience in the field.

Andy Souders

Andy Souders is a technology executive with over 35 years of experience in digital innovation and organizational transformation across industries such as Cloud, Cybersecurity, and Smart Cities. As a three-time CEO and four-time CTO/CIO/CISO, Mr. Souders has led both startups and global enterprises, leveraging strategic planning, product development, and operational excellence with P&L responsibilities over $500M. Currently, Mr. Souders is the CEO, CTO, and Co-Founder of Cybrbase, a cybersecurity assessment platform that enables organizations to measure, optimize, and communicate the maturity of their cybersecurity programs. He is also the Founder and CTO of Think Next Technologies, offering advisory services in emerging tech, and cybersecurity. Additionally, Mr. Souders has held executive roles at All Traffic Solutions, Savi Technology, Clarity Solution Group, and AOL, consistently pioneering advancements in IoT, big data, artificial intelligence, and cybersecurity. A published author and patent holder, Mr. Souders co-founded Pedal It Out, a non-profit supporting cancer awareness and fundraising. Mr. Souders earned his Bachelor of Science degree from Frostburg State University.

MTI FOUNDER

MTI BOARD OF TRUSTEES

Directors

MINETA
TRANSPORTATION
INSTITUTE