

NATIONAL
ACADEMIES

Sciences
Engineering
Medicine

TRB TRANSPORTATION RESEARCH BOARD

TRB Webinar: Cybersecurity Trends in Transportation

November 17, 2022

12:00 – 1:30 PM



AICP Credit Information

1.5 American Institute of Certified Planners Certification Maintenance Credits

You must attend the entire webinar

Log into the American Planning Association website to claim your credits

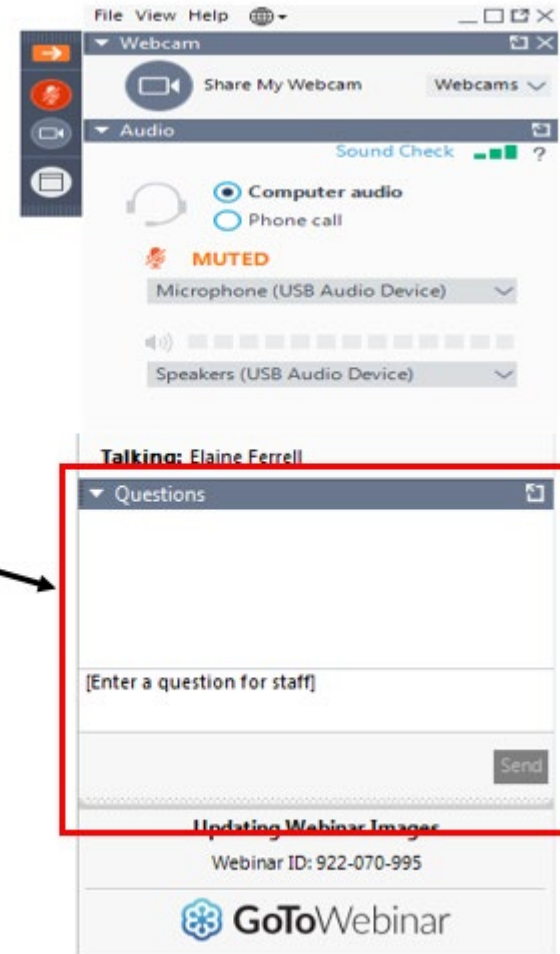
Contact AICP, not TRB, with questions

Learning Objectives

- Improve the cyber resilience of their agency
- Assess cyber risk and cybersecurity at their agency or organization

Questions and Answers

- Please type your questions into your webinar control panel
- We will read your questions out loud, and answer as many as time allows



Today's presenters



David Fletcher

fletcher.d@att.net

Geographic Paradigm Computing, Inc.



Patricia Bye

patriciabye@gmail.com

Independent Consultant



R. Michael Tetreault

roland.tetreault@cisa.dhs.gov

*Cybersecurity & Infrastructure Security
Agency, Department of Homeland
Security*

EMERGING TRENDS IN TRANSPORTATION CYBERSECURITY

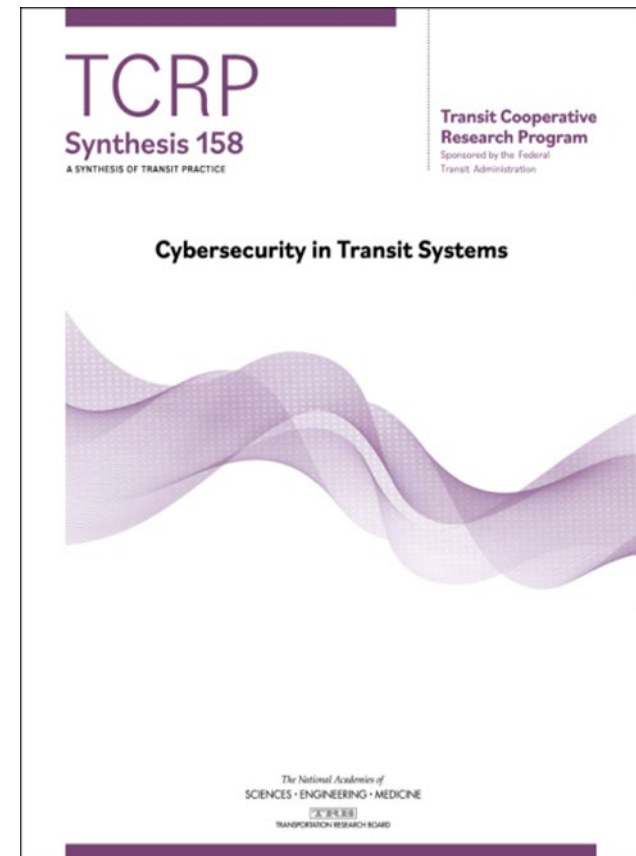
TRB Webinar

November 17, 2022

David Fletcher

Webinar Agenda

- Overview of emerging cybersecurity trends and innovative approaches
- Summary of current state of cybersecurity in transportation
- Updated national cybersecurity trends and the Cybersecurity and Infrastructure Security Agency advisor program



Download the Synthesis:

<https://nap.nationalacademies.org/catalog/26475/cybersecurity-in-transit-systems>

The future is already here; it's just not evenly distributed.

William Gibson (2013)

There are decades where nothing happens;
and then there are weeks where decades
happen.

attributed to Vladimir Lenin (~1913)

Global Cybersecurity Trends

... [P]re-pandemic cybersecurity technologies, approaches and skill sets are no longer adequate to effectively minimize vulnerability, defend against ever-more effective attacks, and rapidly recover and restore agency services and internal operations.

Next-generation cybersecurity approaches are being introduced in other industries and infrastructure sectors and are being promoted by Federal regulators and the cyber insurance industry.

However, agencies report that a lack of funding, the complexity of their existing environments and a lack of expertise are substantial inhibitors to the implementation of these approaches.

Emerging Cybersecurity Trends

- Overview of emerging cybersecurity practice trends across both IT and OT environments, focusing on
 - Focus on cyber resilience, including cyber insurance
 - Third-party cyber risk management, including cyber supply chain risk
 - Cybersecurity of location-agnostic access (e.g., remote work/teleworking/"work-from-home")
 - Zero-trust computing architectures supporting contactless customer applications, including real-time and on-demand information and services
 - Cybersecurity governance and workforce challenges

Cybersecurity and cyber resilience

- “... **cybersecurity** encompasses the combination of policies, business processes and practices, and technologies, designed to protect digital assets (e.g., data, software, systems, networks, and equipment) from unauthorized access, exploitation, damage or loss.
- In contrast, **cyber resilience** refers to a transit agency’s ability to preserve or restore uninterrupted digital services, as expected. These services include both **operational systems** and **information systems**.”

TCRP Synthesis 158

Cyber resilience

Cyber resilience is not a “thing”, but is instead a consequence of political, strategic and operational decisions made by elected officials and senior agency managers that are reflected in agency business policies, plans, processes and workflows. These decisions integrate multiple, often competing and conflicting interests and influences.

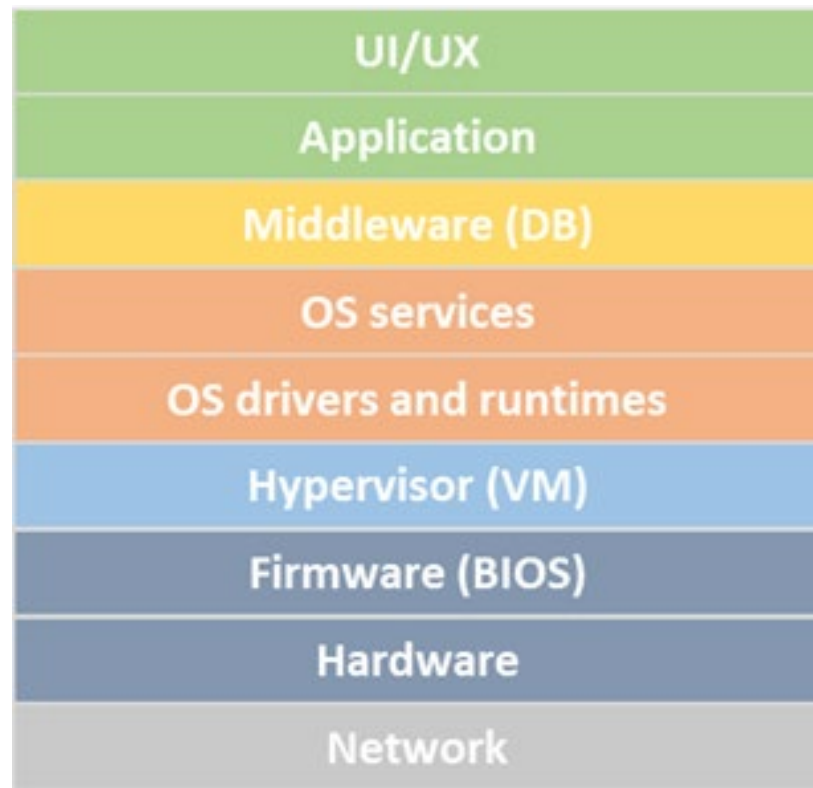


Cyber Insurance Trends

- Finding and negotiating deals is taking longer
- Insurers have less capacity and are providing more restrictive coverages with lower caps
- Deductibles are increasing
- Premiums are rising steeply, in some cases 100% year-over-year
- Many new policies are now excluding ransomware.
- Underwriters are taking a much more aggressive posture in auditing agencies for minimal standards, including adoption of the NIST cybersecurity framework, use of multi-factor authentication, segregated backups, and documented incident response plans. Weak adoption of these practices may result in restricted coverage or in canceled coverage.

IT Supply Chains and Other Risks

- The true risks associated with third and fourth party vendors and digital goods are unknown but assumed to be both large and growing.
- Almost no industry-specific guidance exists to assess, manage and mitigate this risk. Consequently, each agency must perform its own due diligence investigations
- 96% of the software stack use open-source codes



Location-agnostic computing

Employees, suppliers, customers and other stakeholders appear to want to sustain some degree of a new style of working where enterprise data, information services, and cyber resources are accessed, delivered and enabled irrespective of where they are physically located. i.e., anything, anywhere, anytime

The aggregate effect of this demand is to abandon location-centric network architectures where the enterprise controlled the type, configuration, location, access, and security of all of its computing devices for an approach where the employee (and the customer) chooses where their access to enterprise resources happens and increasingly chooses the remote device itself.

Zero-trust computing trends

- “Trust nothing; verify everything.” Access to system resources is strictly limited to only those known/trusted users, systems and networks with an clearly identified and limited need.
- ZT assumes that all environments are inherently risky and that potential attackers can be present in any environment.
- There is no distinction between enterprise environments and non-enterprise ones; the computing environment is continuously monitored and adaptively protected.
- The goals of ZT are twofold 1) prevent unauthorized access to enterprise data, services and resources; and 2) make access decisions and enforcement processes as granular as possible while minimizing transaction costs including authentication (i.e., you are who you say you are) and authorization (i.e., you have permission to use this resource or service) overheads.

Cybersecurity governance trends

1. There is a limited amount of up-to-date, specific cybersecurity guidance available for agencies, particularly as it relates to operational technology.
2. Current metrics used to measure the success of their organization's IT security team are insufficient in a mature cybersecurity-conscious organization.
3. While agency use of cyber insurance is increasing, this tactic may be used to avoid making internal cybersecurity investments. Insurers are aware of this behavior and are raising underwriting requirements and premiums to discourage it.
4. Recruiting, onboarding and retaining qualified cybersecurity employees will continue to be a significant challenge for all organizations. Small and medium sized transit agencies may not be able to successfully compete in this environment and will need to develop more creative and flexible solutions to address this challenge.

Summary of Cybersecurity Trends

1. Very few transportation agencies were planning for or prepared for the scale, scope or timing of the recent digital transformation of the workplace. The ad hoc nature of this transformation exposed or created a number of previously unknown cyber vulnerabilities that in many cases have not yet been identified or mitigated.
2. In many transportation agencies, pre-transformation cybersecurity architectures, policies, training, tools, skillsets, and other resources do not and cannot provide inadequate protection against significant threats.
3. Critical infrastructures, including transportation, are not as reliable, resilient or secure as assumed by elected officials, regulators, operators or customers.
4. As transportation-related services become even more digital, this lack of resilience and security will become even more apparent and may ultimately threaten health and safety, physical assets, and system availability.

THANK YOU

For additional information, contact:
David Fletcher, Principal
Geographic Paradigm Computing, Inc.

CURRENT STATE OF CYBERSECURITY IN TRANSPORTATION

TRB Webinar

November 17, 2022

Pat Bye

Today's Topics

- Cyber vulnerabilities
- Sources and types of cyber incidents
- Cost of cyber incidents
- Cybersecurity guidance available
- Cyber workforce

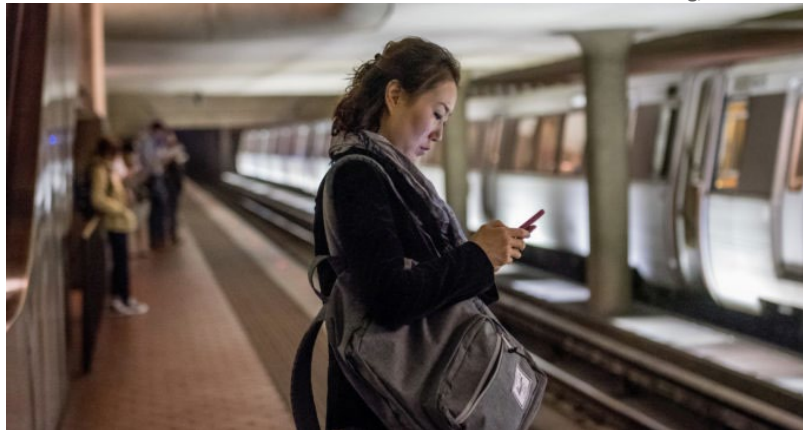
Transit Cyber Vulnerabilities



More Potential Transit Vulnerabilities



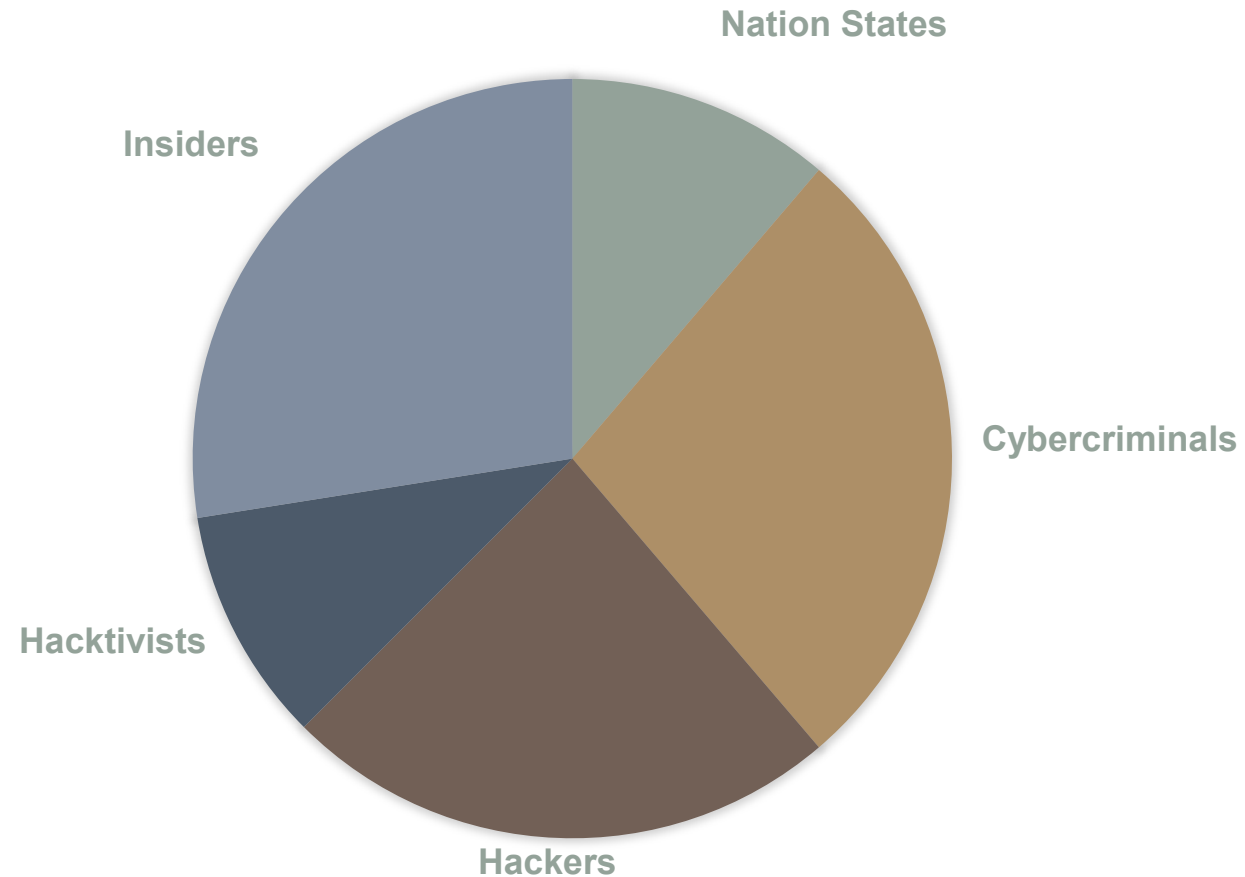
Ben Fractenberg/THE CITY



(Jane Tyska/Bay Area News Group)

Perpetrators of Cyber Incidents

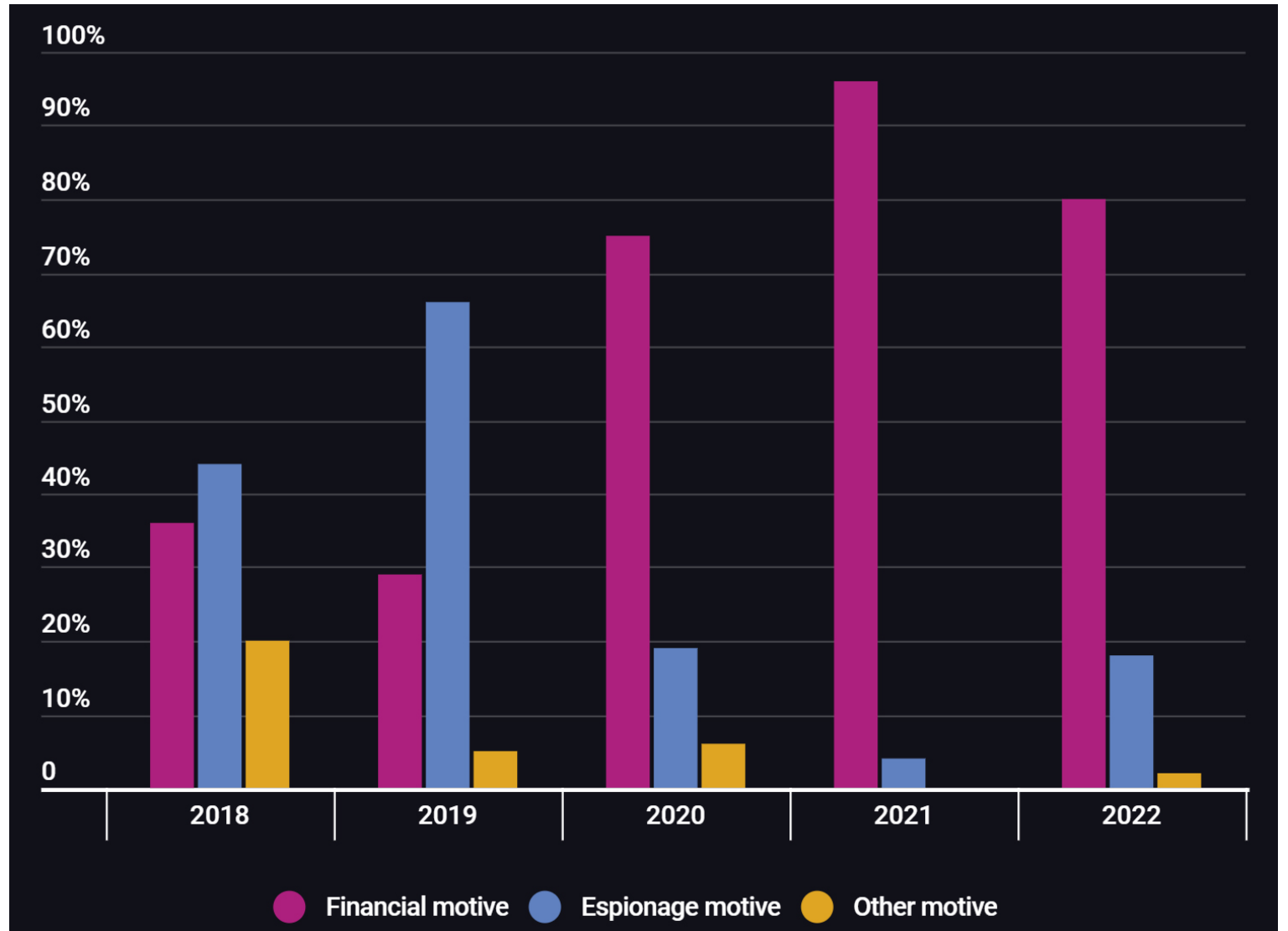
CYBER ACTORS



VALUE CHAIN PROCESS	STATE CYBERTHREAT ACTORS	CYBERCRIMINAL GROUPS	HACKTIVIST GROUPS	INSIDERS
Planning and Scheduling	<ul style="list-style-type: none"> • Theft of intellectual property • Targeted surveillance and monitoring 	<ul style="list-style-type: none"> • Ransomware attacks to disrupt processes for financial gain • Theft of employee PII for sale or extortion 	<ul style="list-style-type: none"> • Disclosures and embarrassment • Theft of travel plans and data • Disruption of expansion • Reputational damage 	<ul style="list-style-type: none"> • Theft of intellectual property • Human error • Insider trading • Data monetization
Pricing and Ticket Sales	<ul style="list-style-type: none"> • Theft of client PII for espionage • Loss or corruption of critical client information • Loyalty or partner network data theft 	<ul style="list-style-type: none"> • Ransomware attacks to disrupt processes for financial gain • Theft of client PII for use or resale • Credit card skimming 	<ul style="list-style-type: none"> • Denial of service attack • Website defacement • Reputational damage 	<ul style="list-style-type: none"> • Disruption or misuse of systems • Human error • Insider trading • Data monetization • Theft of funds
Station Operations (Wi-Fi, maintenance, etc.)	<ul style="list-style-type: none"> • Social disruptions • Interception of public Wi-Fi • Defacement of announcement boards 	<ul style="list-style-type: none"> • Ransomware attacks to disrupt processes for financial gain • Interception of public Wi-Fi 	<ul style="list-style-type: none"> • Disruption of operations through cyber- and physical attacks • Defacement of announcement boards • Reputational damage 	<ul style="list-style-type: none"> • Human error • Disruption of processes • Theft of data or funds • Defacement of announcement boards • Reputational damage
Transit Operations	<ul style="list-style-type: none"> • Theft of system maintenance data • Cyberhijacking • Geolocation data disruptions • Sensor disruptions 	<ul style="list-style-type: none"> • Ransomware attacks to disrupt processes for financial gain 	<ul style="list-style-type: none"> • Disruption of travel • Panic-mongering • Reputational damage 	<ul style="list-style-type: none"> • Disruption of processes • Theft of assets • Human error
Assets and Logistics	<ul style="list-style-type: none"> • Impact on route availability • Social disruption 	<ul style="list-style-type: none"> • Ransomware attacks to disrupt processes for financial gain 		

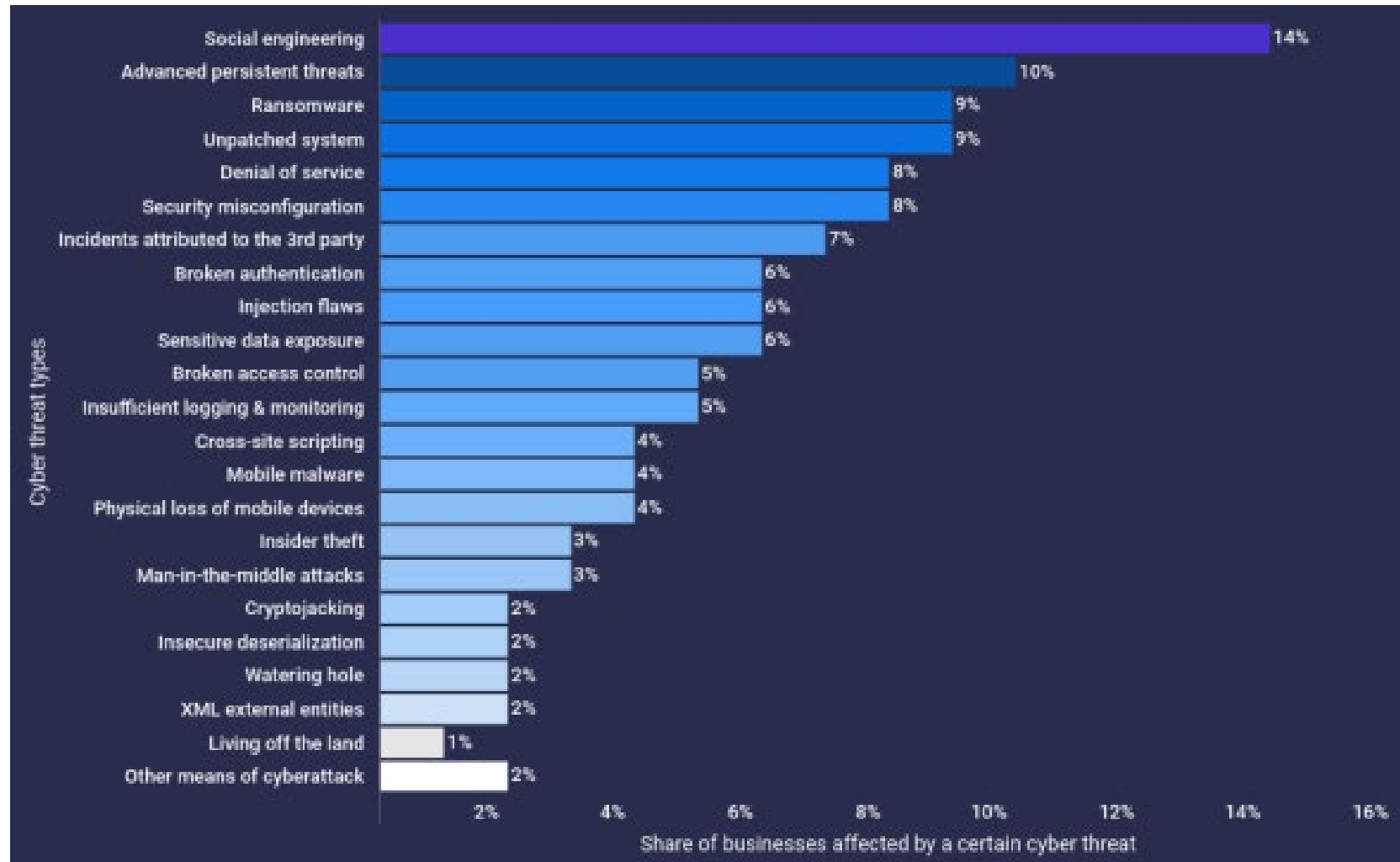
Incident Motive Trends

- Growing financial motivation



Common Types of Incidents

- Many different types
- Most common
 - Ransomware
 - APTs
 - Social Engineering



Planning the Right Zero-Emission Fleet Conversion from the Beginning
 A New Age for Streetcars — AVs Pave the Way to Future Mobility

PAGE 24 PAGE 28

MASS TRANSIT

BEST PRACTICES FOR INTEGRATED MOBILITY

New Ransomware Attacks Pose Costly Threat to Transit Agencies

A more **PROACTIVE** approach to **CYBERSECURITY** can help transit agencies thwart **CYBERCRIMINALS** who are becoming more sophisticated and more organized.

PAGE 14

MassTransitmag.com | November 2020

CYBERSECURITY

Ransomware Attack Shuts Down Several Toronto Transit Commission (TTC) Services

DRIZGROUP.COM @STEVEDRIZ

Valley Regional Transit target of ransomware attack, info may have been compromised

by CBS2 News Staff | Friday, January 21st 2022

Ransomware attack on San Francisco public transit gives everyone a free ride

San Francisco Municipal Transport Agency attacked by hackers who locked up computers and data with 100 bitcoin demand

Ransomware Attacks Montreal Transit System: Cybercriminals Demand \$2.8M

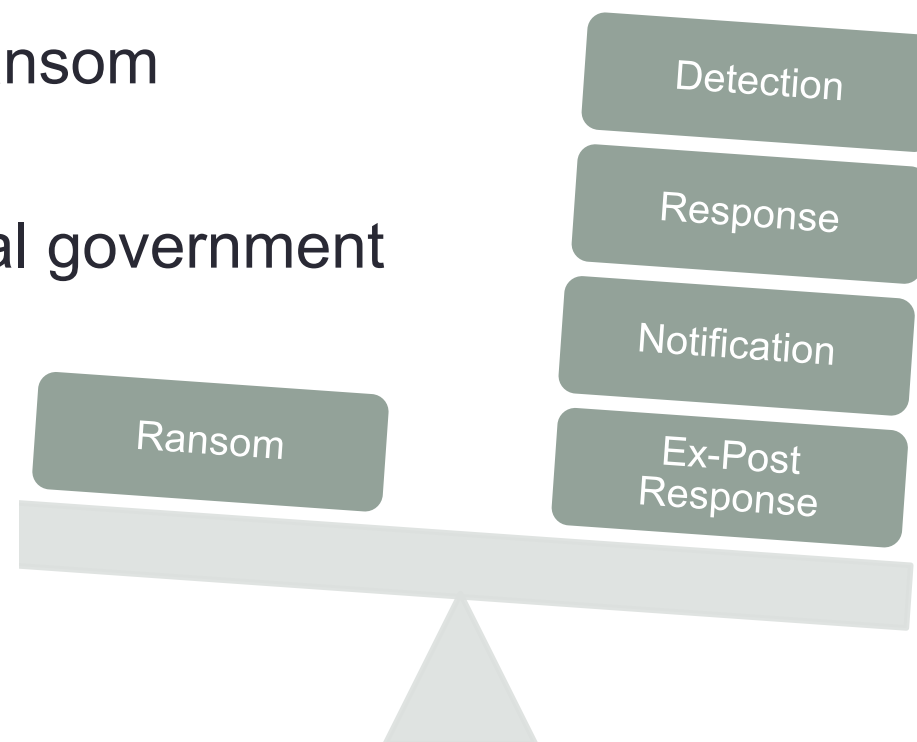
Cybercriminals recently launched a ransomware attack against the Société de transport de Montréal (STM) website & requested a \$2.8 million ransom payment.

Cost of Ransomware

\$4.62 million average cost not including ransom

\$214,000 average ransom in state and local government

34% of those who paid ransom **could not recover data**

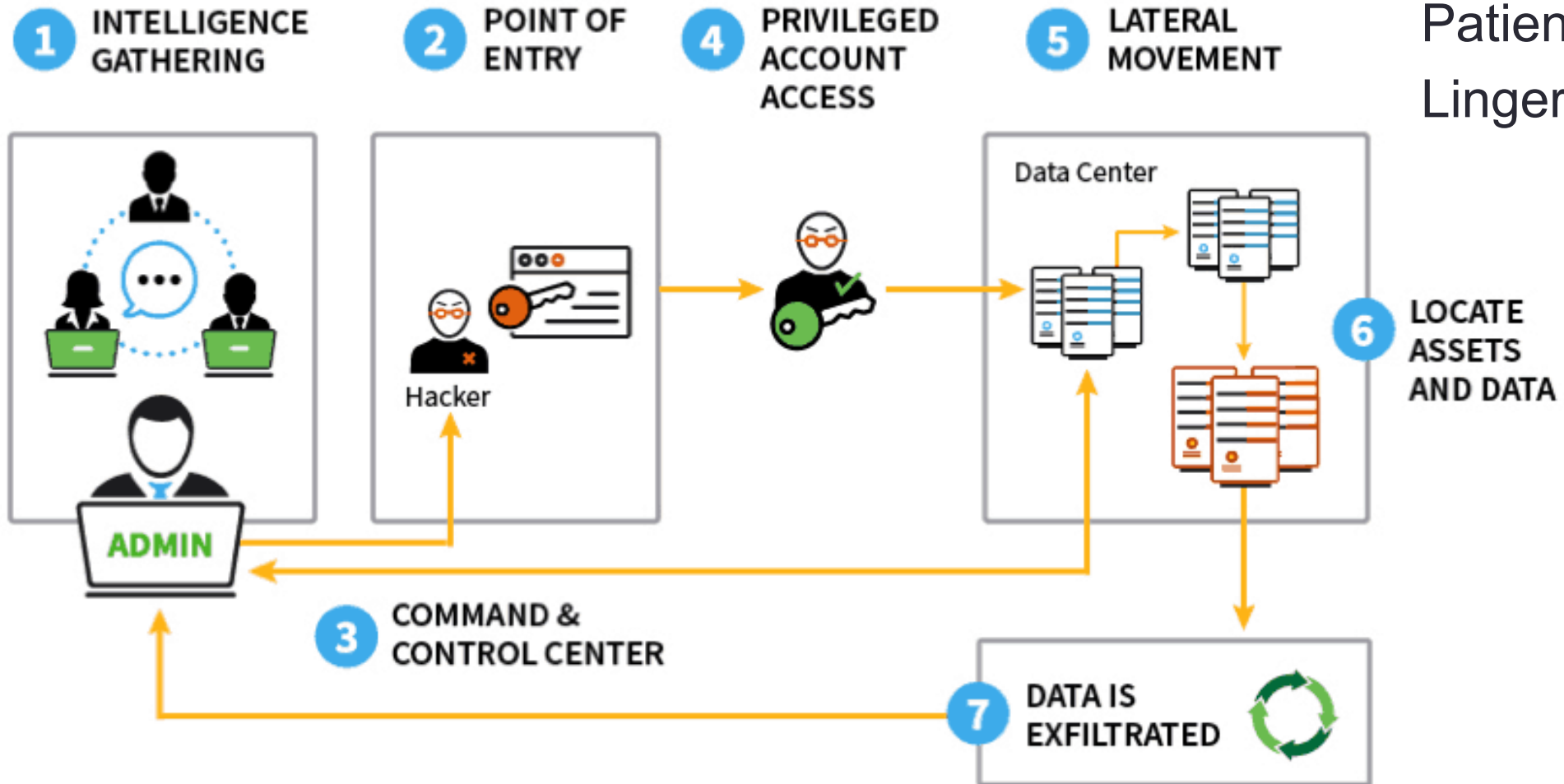


\$3.86 million average cost of recovering from other types of incidents

\$4.24 million average cost of data breach

Public sector data breach costs doubled from \$1M in 2020 to \$2M in 2022

Advanced Persistent Threats (APTs)



Skilled attackers
Patience & Stealth
Linger & Lurk

Social Engineering

Many types including physical breaches

Common types

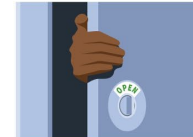
- Phishing
- Email hacking
- Scareware and Baiting
- DNS spoofing



Scareware



Email hacking



Access tailgating



Phishing



DNS spoofing



Baiting



Physical breaches



Pretexting



Watering hole attacks



Quid pro quo

Cybersecurity Guidance

- Rich body from IT perspective
- Growing body for control system cybersecurity



NIST Special Publication 800-82 Revision 2

Guide to Industrial Control Systems (ICS) Security

Supervisory Control and Data Acquisition (SCADA) Systems, Distributed Control Systems (DCS), and Other Control System Configurations such as Programmable Logic Controllers (PLC)

Keith Stouffer
Victoria Pillitteri
Suzanne Lightman
Marshall Abrams
Adam Hahn

TIPS & TACTICS CONTROL SYSTEM CYBERSECURITY



Quick steps you can take now to **PROTECT** your control system:

- 1 PUT SOMEONE IN CHARGE**
Designate one or more people to lead your control system cybersecurity efforts.
- 2 KNOW WHAT YOU HAVE**
Document which types of computer and control system assets you have, how each asset is used, and determine the most critical assets. Check for and remove unauthorized assets.
- 3 ESTABLISH CYBERSECURITY RELATIONSHIPS**
Join your sector-specific cybersecurity communities and establish relationships with vendors and integrators who can help you with recommended cybersecurity practices.
- 4 CHANGE DEFAULT PASSWORDS**
Check your assets for default passwords, and change any you find to new, hard-to-guess passwords. Do not display passwords in plain sight.
- 5 PROTECT ASSETS FROM TAMPERING**
Keep or fiscal assets physically secured and keep the keys of control system assets like Programmable Logic Controllers (PLCs) and safety systems in the "Run" position at all times unless they are being actively programmed.



Additional steps to **MANAGE** your control system cybersecurity risk:

- 1 TRAINING & AWARENESS**
Train control system users on their cybersecurity responsibilities and to look for things out of the ordinary, which may be evidence of a cybersecurity incident.
- 2 MANAGE USER CREDENTIALS & ACCESS**
Check who has on-site or remote access to your systems, and revoke access that isn't needed. Immediately disable accounts and revoke ID when someone leaves the organization.
- 3 RESTRICT ACCESS TO THE CONTROL SYSTEM NETWORK & NETWORK ACTIVITY**
Implement layered network topology with Demilitarized Zone (DMZ) to restrict access to control system networks. Restrict control system access to only user-situated equipment. Consider requiring two-factor authentication for remote access instead of only a password.
- 4 MANAGE CYBERSECURITY VULNERABILITIES**
Keep your assets up-to-date and fully patched. Prioritize patching of "PC" machines used in Human Machine Interfaces (HMI), database servers, and engineering workstations. Disable unused ports and services. Implement anti-virus and malware scanning technologies where feasible to prevent, detect, and mitigate malware including ransomware.
- 5 IMPLEMENT APPLICATION CONTROL**
The strict nature of some control system assets, such as database servers, HMIs, and engineering workstations make them ideal candidates to run application control solutions.
- 6 PREPARE TO RECOVER FROM A CYBERSECURITY INCIDENT**
Develop and implement an incident recovery plan. Plan, implement, and test a system and data backup and restoration strategy.
- 7 IMPLEMENT & PERFORM CONTINUOUS MONITORING**
Continuously monitor system boundaries and ingress and egress traffic. Be aware of relevant cybersecurity threats and vulnerabilities by using free resources like those available from NIST and the Cybersecurity & Infrastructure Security Agency (CISA).



TIPS & TACTICS RANSOMWARE



Quick steps you can take now to **PROTECT** yourself from the threat of ransomware:

- 1 USE ANTIVIRUS SOFTWARE AT ALL TIMES**
Set your software to automatically scan emails and flash drives.
- 2 KEEP YOUR COMPUTER FULLY PATCHED**
Run scheduled checks to keep everything up-to-date.
- 3 BLOCK ACCESS TO RANSOMWARE SITES**
Use security products or services that block access to known ransomware sites.
- 4 ALLOW ONLY AUTHORIZED APPS**
Configure operating systems or use third party software to allow only authorized applications on computers.
- 5 RESTRICT PERSONALLY-OWNED DEVICES**
Organizations should restrict or prohibit access to official networks from personally-owned devices.
- 6 USE STANDARD USER ACCOUNTS**
Use standard user accounts vs. accounts with administrative privileges whenever possible.
- 7 AVOID USING PERSONAL APPS**
Avoid using personal applications and websites – like email, chat, and social media – from work computers.
- 8 BEWARE OF UNKNOWN SOURCES**
Don't open files or click on links from unknown sources unless you first run an antivirus scan or look at links carefully.



Steps you can take now to help you **RECOVER** from a future ransomware attack:

- 1 MAKE AN INCIDENT RECOVERY PLAN**
Develop and implement an incident recovery plan with defined roles and strategies for decision-making.
- 2 BACKUP & RESTORE**
Carefully plan, implement, and test a data backup and restoration strategy – and secure and isolate backups of important data.
- 3 KEEP YOUR CONTACTS**
Maintain an up-to-date list of internal and external contacts for ransomware atacks, including law enforcement.



Transit Cybersecurity Guidance



APTA SS-ECS-RP-001-14, Rev. 1

First Published: Oct. 17, 2014

First Revision: July 29, 2022

American Public Transportation Association
1300 I Street, NW, Suite 1200 East, Washington, DC 20006

Enterprise Cyber Security Working Group



APTA SS-CCS-WP-005-19

First Published: July 7, 2019

Control and Communications Security Working Group



APTA STANDARDS DEVELOPMENT PROGRAM
RECOMMENDED PRACTICE

American Public Transportation Association
1666 K Street, NW, Washington, DC, 20006-1215

APTA SS-CCS-RP-001-10

Approved: IT Policy & Planning Committee July 30, 2010

APTA Control and Communications Working Group

Cybersecurity Considerations for Public Transit

Abstract: This recommended practice establishes considerations for public transit chief information officers interested in developing cybersecurity strategies for their organizations. It details practices and standards that address vulnerability assessment and mitigation, system resilience and redundancy, and disaster recovery.

Keywords: advanced persistent attacks, cyber, cyber-assets, cybersecurity assessments, disaster recovery, enterprise cybersecurity, fallback, information security (INFOSEC), information and communication technology (ICT), information security, intrusion detection, redundancy, resilience, secure cloud, system penetration.

Summary: Cybersecurity is a growing concern for public transit managers, as control and management systems become increasingly dependent on information technology. These systems are vulnerable to increasingly sophisticated direct and indirect cyberattacks. The typical transit-based IT infrastructure comprises complex and interconnected components, subcomponents, and services. This complexity increases the exposure of these systems to threats. Given these increasing risks, the transit industry and its technology managers must take proper steps to ensure the security of their cybersystems. Working remotely has increased the risk of compromising electronic security perimeters. Transit organizations must prioritize cybersecurity control implementation and ongoing operations management.

Scope and purpose: This document provides information on and considerations for cybersecurity within the public transit industry and enterprise. This document is not a substitute for implementing a formal cybersecurity program or cybersecurity framework. Nothing in this document is intended to contradict mandatory local, state or federal governments' standards or guidelines.

This document represents a common viewpoint of those parties concerned with its provisions, namely transit operating/planning agencies, manufacturers, consultants, engineers and general interest groups. The application of any recommended practices or guidelines contained herein is voluntary. APTA standards are mandatory to the extent incorporated by an applicable statute or regulation. In some cases, federal and/or state regulations govern portions of a transit system's operations. In cases where there is a conflict or contradiction between an applicable law or regulation and this document, consult with a legal adviser to determine which document takes precedence.

© 2022 The American Public Transportation Association (APTA). No part of this publication may be reproduced in any form, in an electronic retrieval system or otherwise, without prior written permission of APTA.

Securing Control and Communications Systems in Transit Bus Vehicles and Supporting Infrastructure

Abstract: This white paper presents an overview of transit bus cybersecurity issues and a preliminary look at some methodologies that may be used for risk assessments on transit bus systems.

Keywords: cybersecurity, risk assessment, transit bus, transportation security

Summary: This document provides control and communications security systems designed to protect a transit agency's transit bus infrastructure, including vehicles, communications channels, control room, remote access data processing facilities and maintenance garages.

Scope and purpose: This white paper is not intended to supplant existing safety/security standards or regulations but to supplement them with additional guidance. The purpose of this white paper is to share transit agency best practices; to present a view of threats and evaluation techniques for control security within the bus transit industry, with the aim of documenting voluntary industry practices in control security in advance of, and in coordination with, government regulation, and to raise awareness of control security concerns and issues in the industry.

This document represents a common viewpoint of those parties concerned with its provisions, namely transit operating/planning agencies, manufacturers, consultants, engineers and general interest groups. The application of any recommended practices or guidelines contained herein is voluntary. APTA standards are mandatory to the extent incorporated by an applicable statute or regulation. In some cases, federal and/or state regulations govern portions of a transit system's operations. In cases where there is a conflict or contradiction between an applicable law or regulation and this document, consult with a legal advisor to determine which document takes precedence.

© 2019 The North American Transportation Services Association (NATSA) and its parent organization APTA. No part of this publication may be reproduced in any form, in an electronic retrieval system or otherwise, without prior written permission of NATSA.

Securing Control and Communications Systems in Transit Environments

Part 1: Elements, Organization and Risk Assessment/Management

Previously numbered as APTA-RP-CCS-1-RT-001-10

Abstract: This document covers recommended practices for securing control and communications systems in transit environments.

Keywords: control and communications security, cyber-security, radio, SCADA, train control

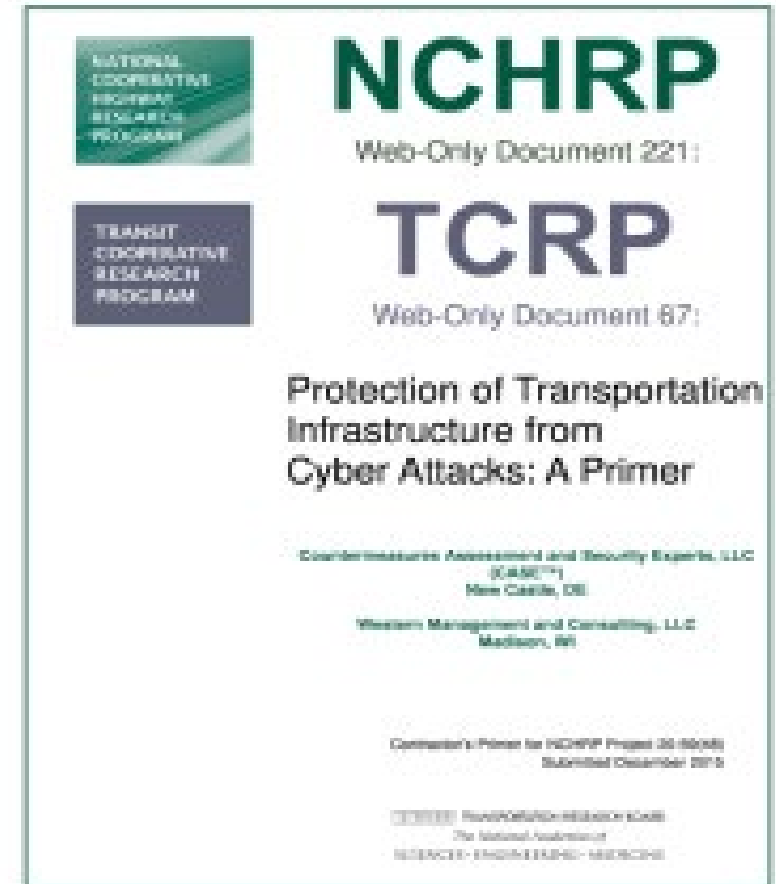
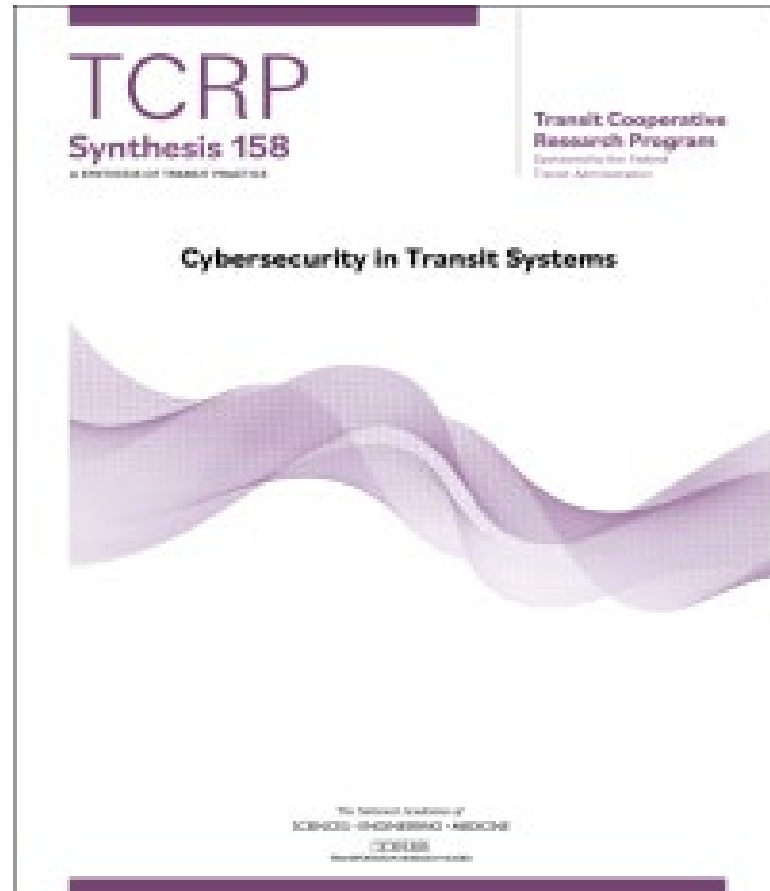
Summary: This *Recommended Practice* addresses the importance of control and communications security to a transit agency, provides a survey of the various systems that constitute typical transit control and communication systems, identifies the steps that an agency would follow to set up a successful program, and establishes the stages in conducting a risk assessment and managing risk.

Scope and purpose: This document addresses the security of the following passenger rail and/or bus systems: SCADA, traction power control, emergency ventilation control, alarms and indications, fire/intrusion detection systems, train control/signaling, fare collection, automatic vehicle location (AVL), physical security feeds (CCTV, access control), public information systems, public address systems, and radio/wireless/related communication. In the event that security/safety or other standards exist for any of the above systems, this *Recommended Practice* will supplement, provide additional guidance for, or provide guidance on how control systems may securely interface with these systems. While the agency's network infrastructure may be used for multiple purposes, this *Recommended Practice* includes protection of any control information that is communicated across the agency's network.

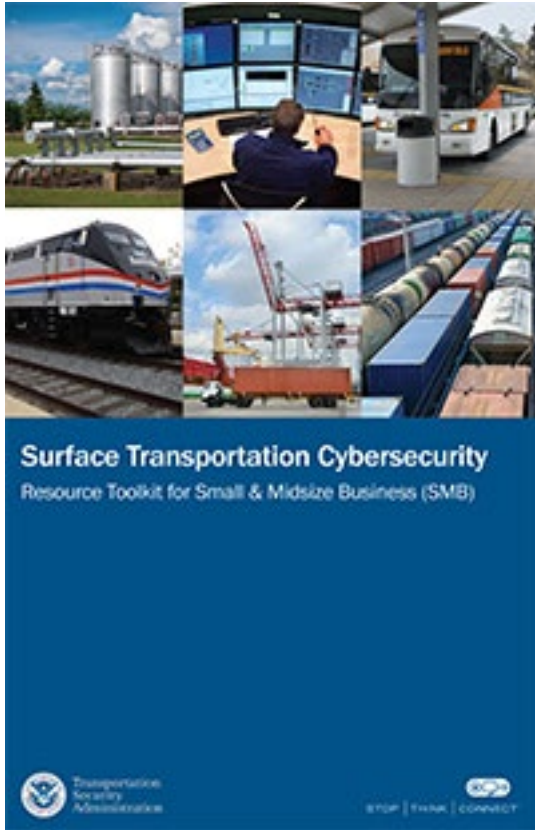
Passenger transit agencies and the vendor community now evolve their security requirements and system security features independently for most of the systems listed above. The purpose of this *Recommended Practice* is to share transit agency best practices; set a minimum requirement for control security within the transit industry; provide a guide of common security requirements to control and operations systems vendors; adopt voluntary industry practices in control security in advance and in coordination with government regulation; and raise awareness of control security concerns and issues in the industry.

This Recommended Practice represents a common viewpoint of those parties concerned with its provisions, namely, transit operating/planning agencies, manufacturers, consultants, engineers and general interest groups. The application of any standards, practices or guidelines contained herein is voluntary. In some cases, federal and/or state regulations govern portions of a rail transit system's operations. In those cases, the government regulations take precedence over this standard. APTA recognizes that for certain applications, the standards or practices, as implemented by individual rail transit agencies, may be either more or less restrictive than those given in this document.

Transit Cybersecurity Guidance



DHS/CISA Transportation Guidance



Transportation Systems Sector Cybersecurity Framework Implementation Guidance

NIST Framework Implementation Guidance Cycle



STOP RANSOMWARE

RESOURCES NEWSROOM ALERTS REPORT RANSOMWARE CISA.GOV

Daixin Team
Leverages Ransomware to Target the Healthcare and Public Health Sector

HAVE YOU BEEN HIT BY RANSOMWARE?
LEARN MORE

Known Exploited Vulnerabilities Catalog
Updated

RANSOMWARE

Protection and Response **Services** **Public Safety** **Preparation**

Ransomware is a form of malware designed to encrypt files on a device, rendering any files and the systems that rely on them unusable. Malicious actors then demand ransom in exchange for decryption. Stopransomware.gov is the U.S. Government's official one-stop location for resources to tackle ransomware more effectively.

HOW WE CAN HELP
General Information
FAQs
Tips
Ransomware Readiness Self-Assessment

GUIDANCE AND RESOURCES
Ransomware is an ever-evolving form of malware designed to encrypt files on a device, rendering any files and the systems that rely on them unusable. Malicious actors then demand ransom in exchange for decryption. These resources are designed to help individuals and organizations prevent attacks that can severely impact business processes and leave organizations without the data they need to operate and deliver mission-critical services.

TIPS & GUIDANCE
Ransomware incidents can severely impact business processes and leave organizations without the data they need to operate and deliver mission-critical services. The economic and reputational impacts of ransomware incidents, throughout the initial disruption and, at times, extended recovery, have also proven challenging for organizations large and small. Apply these tips and practices to avoid attack.

Good Cyber Hygiene Habits Keep Your Network Healthy
Conduct regular vulnerability scanning to identify and address vulnerabilities, especially those on internet.

When in Doubt, Report It Out
Victims of ransomware should report to federal law enforcement via ICS or a Secret Service Field Office, and can request technical assistance or provide information.

“Cybersecurity is not a priority in many transit agencies as evidenced by the lack of investment or additional staffing.”

2020 SJSU/MTI Survey

Project 1939 | August 2020

SJSU SAN JOSÉ STATE UNIVERSITY

MTI MINETA TRANSPORTATION INSTITUTE

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

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



MINETA TRANSPORTATION INSTITUTE transweb.sjsu.edu

Project 2111 | July 2020

SJSU SAN JOSÉ STATE UNIVERSITY

MTI MINETA TRANSPORTATION INSTITUTE

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

Scott Belcher, Terri Belcher, Eric Greenwald, Brandon Thomas, William Singh



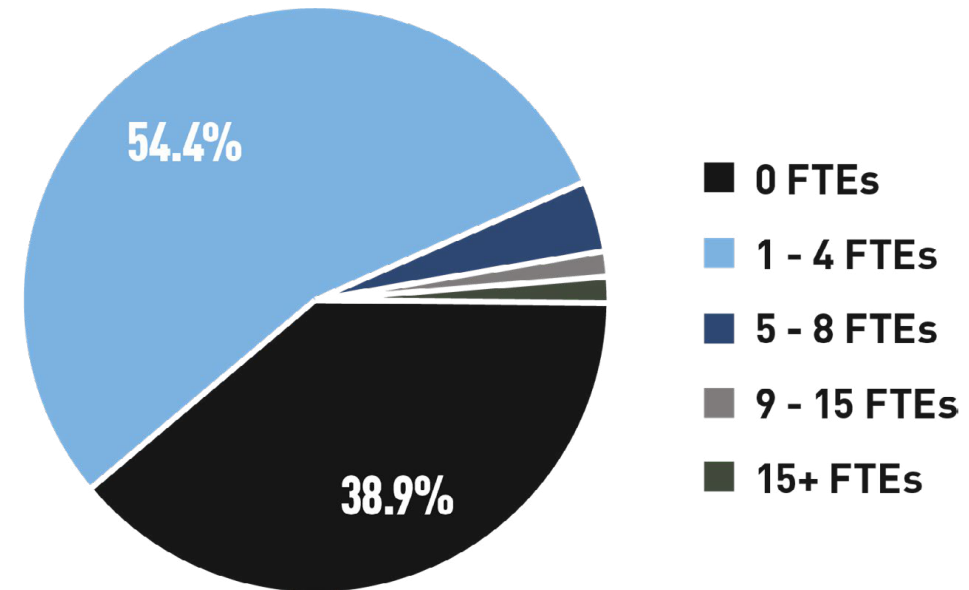
MINETA TRANSPORTATION INSTITUTE transweb.sjsu.edu

Transit Cybersecurity Staffing

Levels are low relative to other industries

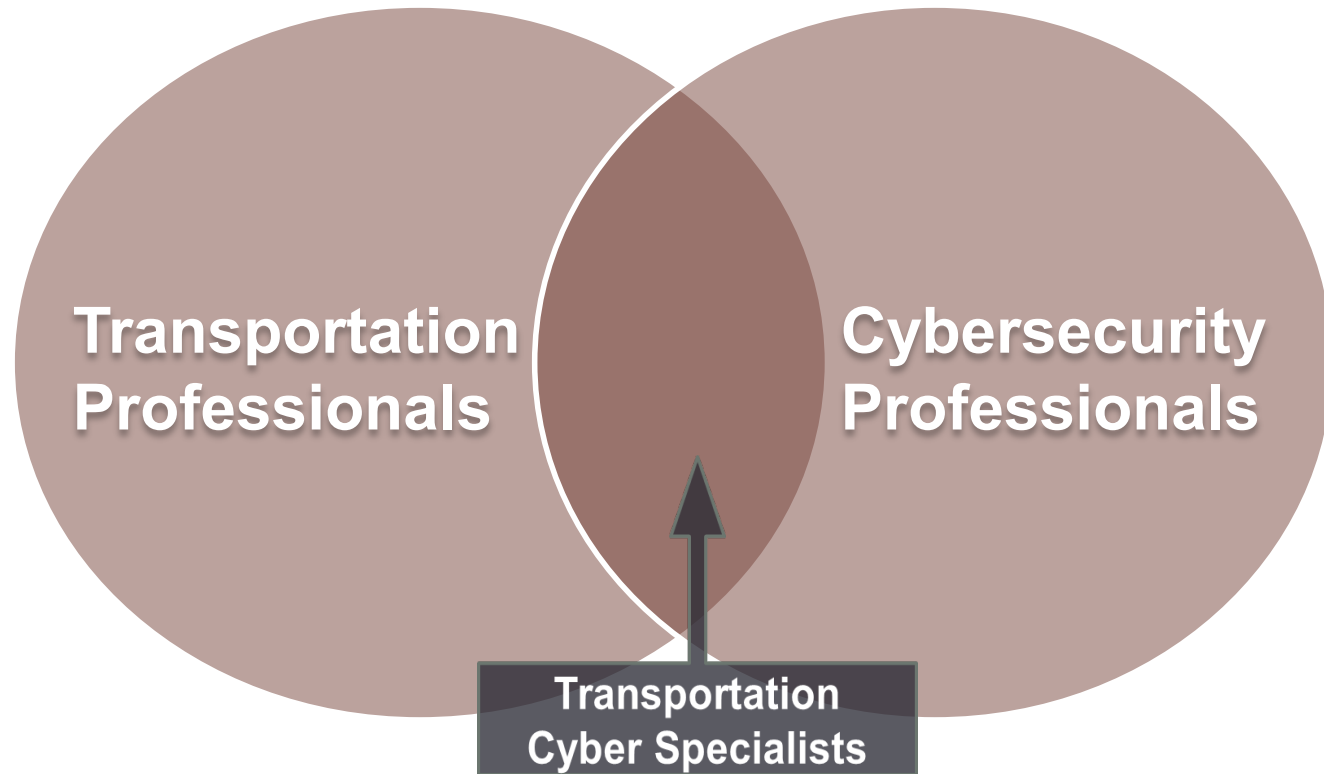
Does not correlate with

- agency size
- whether agency reported having incident



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

Transit Agency Skills Gap



THANK YOU

For additional information, contact:

Pat Bye

patriciabye@gmail.com

U.S. Department of Homeland Security

CYBERSECURITY AND INFRASTRUCTURE SECURITY AGENCY

DEFEND TODAY,
SECURE TOMORROW



R. MIKE TETREAU

Cybersecurity Advisor, Region I (RI)

Cybersecurity and Infrastructure Security Agency (CISA)

Our Work

The Cybersecurity and Infrastructure Security Agency (CISA) is the Nation's risk advisor, working with partners to defend against today's threats and collaborating to build more secure and resilient infrastructure for the future



PARTNERSHIP
DEVELOPMENT



INFORMATION AND
DATA SHARING



CAPACITY BUILDING



INCIDENT
MANAGEMENT
& RESPONSE



RISK ASSESSMENT
AND ANALYSIS



















NETWORK DEFENSE



EMERGENCY
COMMUNICATIONS

16 Critical Infrastructure Sectors & Corresponding Sector Risk Management Agencies

 CHEMICAL	CISA	 FINANCIAL	Treasury
 COMMERCIAL FACILITIES	CISA	 FOOD & AGRICULTURE	USDA & HHS
 COMMUNICATIONS	CISA	 GOVERNMENT FACILITIES	GSA & FPS
 CRITICAL MANUFACTURING	CISA	 HEALTHCARE & PUBLIC HEALTH	HHS
 DAMS	CISA	 INFORMATION TECHNOLOGY	CISA
 DEFENSE INDUSTRIAL BASE	DOD	 NUCLEAR REACTORS, MATERIALS AND WASTE	CISA
 EMERGENCY SERVICES	CISA	 TRANSPORTATIONS SYSTEMS	TSA & USCG
 ENERGY	DOE	 WATER	EPA

**SEE YOURSELF
IN CYBER**



Key Concepts

- People, Process and Technology
- Confidentiality, Integrity & Availability
- Leadership and Policy are essential
- Resilience & Risk Management
(Risk = Threats * Vulnerabilities)
- There is no “silver bullet”! It is a team effort!



- **Cybersecurity Myths**

- You can write a check for resilience. False!
- Cyber Insurance is a cyber security program. False!
- Cloud based does not need cybersecurity! False!



Action Steps



Our goal is to have everyone implement these four action steps to increase online security:

- **Enable Multi-Factor Authentication:** You need more than a password to protect your online accounts, and enabling MFA makes it 99% less likely you will get hacked
- **Use Strong Passwords:** Use passwords that are long, unique, and randomly generated.
- **Recognize and Report Phishing:** If a link looks a little off, think before you click. It could be an attempt to get sensitive information or install malware.
- **Update Your Software:** Don't delay – if you see a software updated notification, act promptly. Better yet, turn on automatic updates.



SHIELDS UP



Latest Updates

Guidance for All organizations

- Reduce the likelihood of a damaging cyber intrusion
- Take steps to quickly detect a potential intrusion
- Ensure that the organization is prepared to respond if an intrusion occurs
- Maximize the organization's resilience to a destructive cyber incident

Recommendations for Corporate Leaders and CEOs

- Empower the Chief information Security Officer (CISO)
- Lower Reporting Thresholds
- Participate in a Test of Response Plans
- Focus on Continuity
- Plan for the Worst



SHIELDS UP



Ransomware Response - CISA

- Checklist
- Ransomware Guide
- StopRansomware.gov
- StaySafeOnline.org
- I've Been Hit by Ransomware! page

Steps You Can Take to Protect Yourself & Your Family

- Implement multi-factor authentication
- Update your software
- Think before you click
- Use strong passwords

Additional Resources: Cybersecurity Advisories, Preparedness Tools, CISA Tools, Mal-information and Emergency Communications

Mike Tetreault – RI CSA
Tuesday, November 15, 2022



Cyber Resource Hub

- Assessments and Evaluations
- Vulnerability Scanning
- Cyber Resilience Review & Downloadable Resources
- External Dependency Management & Downloadable Resources
- Cyber Infrastructure Survey
- Web Application Scanning
- Cyber Security Evaluation Tool (CSET)
- Free Public and Private Sector Tools and Services



Training & Exercises

Critical Infrastructure Entities

- Assessment Evaluations and Standardization
- Continuous Diagnostics and Mitigation
- CISA Tabletop Exercise package
- Industrial Control Systems

Cybersecurity Professionals & General Public

- Cybersecurity Exercises
- Federal Virtual Training Environment (FedVTE)
- Certification Preparation
- NICE Cybersecurity Framework
- Workforce Training Guides
- Incident Response Training



Get Started Today!

R. Mike Tetreault

Cybersecurity

Advisor for RI

roland.tetreault@cisa.dhs.gov

Cell: 202-941-1288



Today's presenters



David Fletcher

fletcher.d@att.net

Geographic Paradigm Computing, Inc.



Patricia Bye

patriciabye@gmail.com

Independent Consultant



R. Michael Tetreault

roland.tetreault@cisa.dhs.gov

*Cybersecurity & Infrastructure Security
Agency, Department of Homeland
Security*

Upcoming events for you

December 12, 2022

TRB Webinar: Expanding
Microtransit Services and Improving
the Rider Experience

December 13, 2022

TRB Webinar: Trends in Transit
Ridership—Analysis, Causes, and
Responses

[https://www.nationalacademies.org/trb/
events](https://www.nationalacademies.org/trb/events)



Register for the 2023 TRB Annual Meeting



Register to be part
of the **action!**



Scan me

<https://www.trb.org/AnnualMeeting/Registration.aspx>

Follow the conversation
#TRBAM

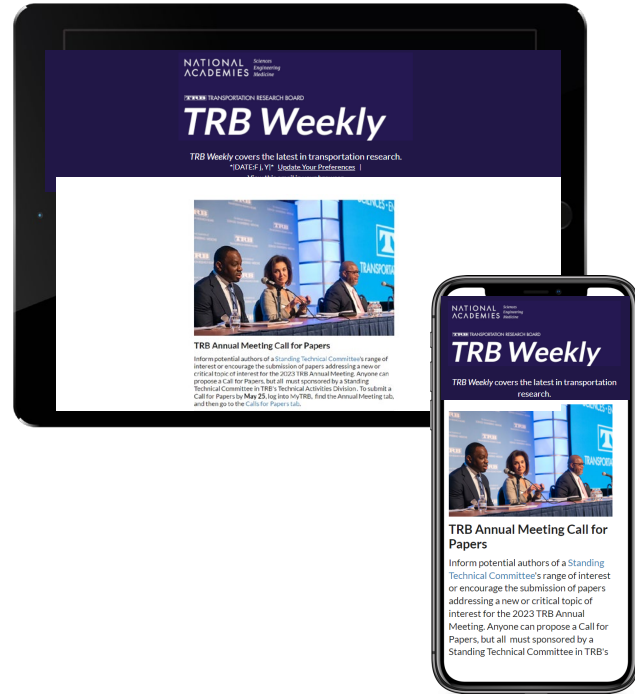
NATIONAL
ACADEMIES *Sciences
Engineering
Medicine*

Subscribe to *TRB Weekly*

If your agency, university, or organization perform transportation research, you and your colleagues need the *TRB Weekly* newsletter in your inboxes!

Each Tuesday, we announce the latest:

- RFPs
- TRB's many industry-focused webinars and events
- 3-5 new TRB reports each week
- Top research across the industry



Spread the word and subscribe!

<https://bit.ly/ResubscribeTRBWeekly>

Discover new TRB Webinars weekly

Set your preferred topics to get the latest listed webinars and those coming up soon every Wednesday, curated especially for you!

<https://mailchi.mp/nas.edu/trbwebinars>

And follow #TRBwebinar on social media



Get involved

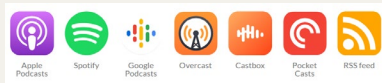
<https://www.nationalacademies.org/trb/get-involved>

- **Become a Friend of a Standing Technical Committee**

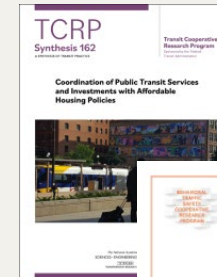
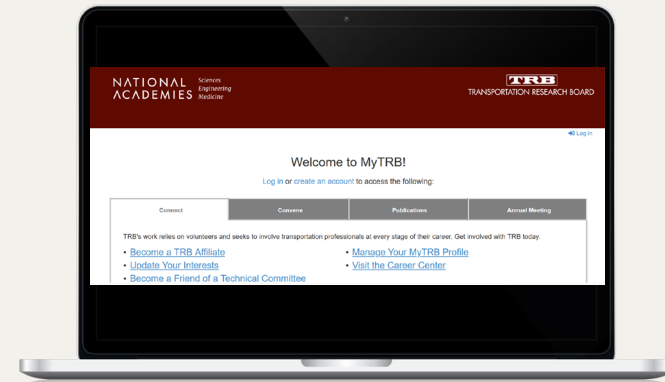
Network and pursue a path to Standing Committee membership

- **Work with a CRP**

- **Listen to our podcast**



<https://www.nationalacademies.org/podcasts/trb>



We want to hear from you

- Take our survey
- Tell us how you use **TRB Webinars** in your work at trbwebinar@nas.edu

