Transportation Security Administration

EXIS | Exercise Information System

American Bus Association - Cybersecurity TTX After Action Report

July 23, 2024 | Orlando, FL

This document was created in EXIS® on 7/29/2024 and last modified on 7/29/2024.

Table of Contents

Administrative Handling Instructions

This document should be safeguarded, handled, transmitted, and stored in accordance with TSA directives. It should be released to individuals on a strict need-to-know basis. Information contained herein was prepared for the exclusive use of Planning Team members, project officers, and non-participant personnel involved in the operational and administrative aspects of the exercise. The contents of this handbook will not be divulged to non-exercise Participants unless officially authorized by TSA. Reproduction of this document, in whole or in part, without prior written approval from TSA is prohibited.

Intermodal Security Training and Exercise Program

The Transportation Security Administration's (TSA) Intermodal Security Training and Exercise Program (I-STEP) provides exercise, training, and security planning tools and services to the transportation community. The program focuses on the security nexus of the intermodal transportation environment, serving mass transit, freight rail, pipeline, port and intermodal, highway and motor carrier, and aviation modes. Working in partnership with the transportation modes, I-STEP enables security partners to:

- Enhance security capabilities - Strengthen plans, policies, and procedures; clarify roles and responsibilities; validate planning needs; and strengthen grant proposals.
- Build partnerships - Develop relationships with regional transportation players and other stakeholders.
- Gain insights in transportation security - Network with peers to gain a deeper understanding of security lessons learned and best practices.

I-STEP is the only Federal exercise program to focus on the security nexus of the intermodal transportation environment. As a result, the program reduces risk to individual systems as well as the entire transportation network. I-STEP aligns to TSA's Transportation Systems Sector-Specific Plans (TSSSP) under the National Infrastructure Protection Plan (NIPP). TSA's Policy, Plans, and Engagements (PPE) manages this program. The Exercise Information System (EXIS) portal guides users through a step-by-step exercise planning process to develop their own specific security exercise. EXIS is an intuitive system providing a variety of exercise planning and evaluation tools as well as lessons learned and best practices from the DHS Transportation Systems Sector and other aligned user communities. Lessons learned and best practices from exercises and training events along with intelligence information help shape transportation security policy and guidance. Go to: https://exis.tsa.dhs.gov to receive an account and use the tool.

I-STEP Programmatic Goals

- Develop a comprehensive transportation security exercise program
- Serve as a training resource for TSA security partners
- Foster information sharing/collaboration among security partners
- Provide support services to TSA modal representatives

Point of contact

I-STEP Program Office
istep@tsa.dhs.gov

Exercise Overview

Purpose and Scope

The purpose of this exercise is to provide the bus industry owners and operators the opportunity to review operational and security procedures that guide information sharing, IT networks and OT networks, implementation of physical protective measures, and operational coordination among industry employees, industry partners, and security stakeholders in the event of a cybersecurity incident.

Objectives

Mission Area	Core Capability	Objective
Prevention	Intelligence and Information Sharing	Review and evaluate plans and capabilities that support the collection, analysis, and dissemination of intelligence about cybersecurity threats to local transportation operators and security stakeholders.
Protection	Cybersecurity	Assess how operators and stakeholders select, resource, share, and implement risk-based protective measures following a cybersecurity threat. Discuss physical and cybersecurity measures currently in place to protect the industry; identify wants, needs and desires.
Recovery	Planning	Discuss how transportation operators, stakeholders, and federal agencies can coordinate and communicate following a coordinated cyberattack

Scenario

An unknown cyberattack has occurred after an employee opens an email containing a phishing/ DDOS attack.

See Full Scenario listed below

Outcomes

Strengths

- Majority of the representatives at the exercise receive information from federal, state and local partners via Informational Bulletins and other information shared; the few organizations that don't receive the information believed they didn't have a need however they signed up or will sign up.
- Participants identified they have either internal or a 3rd party resource able to help them with cybersecurity issues when it directly impacts them. They also require all employees to take internal cybersecurity training should an incident occur.
- Participants identified they are actively using their immediate resources to handle and mitigate cybersecurity threats. The usage of internal or 3rd party IT has proven to be the most beneficial aspect; however, they continue to feel that there is insufficient information being shared due to sensitivity considerations.
- A select few participants identified times they have reached out to other organizations or federal partners to obtain additional information and/or asked their respective IT department or 3rd party entity to obtain additional information to cybersecurity attacks.

Areas for Improvement

- Organizations represented at the exercise realized while they did have people who receive the information there is no onboarding process requiring people to sign up to receive information from respective partners. The Association identified a need to bring federal partners to their regular meetings – when possible – to provide a current level of the threat awareness.
- While they do have policies, procedures and systems in place, participants identified they don't actively engage with their IT department or 3rd party resource for identification of what has occurred in other parts of the transportation sector. They identified they aren't fully using all the resources offered by the federal government to include TSA and CISA.
- The need to establish a physical understanding when a cybersecurity incident occurs is important. It was identified in the event of a cybersecurity incident multiple systems could be impacted thus creating a physical demand as organizations would return back to paper copies and potential for issues from paying drivers to scheduling and tracking when present a critical failure within the organization. Historical information – paper copies – has not been dusted off or refreshed as everything is on computer system but the need to create redundancies in the system has proven relevant.
- Multiple organizations didn't know all the offerings from federal partners and requested additional information. Certain participants stated they wouldn't know who to call in the event of an incident beyond their insurance company and respective IT support (3rd party or internal) to help remedy the situation. One organization identified their leadership team wears multiple hats so their only solution is external support, and it would be focused on the response phase to get back up and running compared to preemptive or sustainment.

Exercise Data Capture and Analysis

Objective 1: *Met*

Review and evaluate plans and capabilities that support the collection, analysis, and dissemination of intelligence about cybersecurity threats to local transportation operators and security stakeholders.

Objective Summary

Participants discussed how the currently receive information pertaining to cybersecurity and the transportation system sector, additional discussion on usage of social media platforms and mass media to better enhance their response capabilities - routing planning and diversion considerations.

STRENGTH

1. **Strength:** Majority of the representatives at the exercise receive information from federal, state and local partners via Informational Bulletins and other information shared; the few organizations that don't receive the information believed they didn't have a need however they signed up or will sign up.

   Benefit Analysis

   When organizations begin to receive more information, they are adequately able to be prepared when the threat environment changes and take additional actions into considerations.

   References

   TSA SISC & CISA Cyber Hygiene

AREA FOR IMPROVEMENT

1. **Area For Improvement:** Organizations represented at the exercise realized while they did have people who receive the information there is no onboarding process requiring people to sign up to receive information from respective partners. The Association identified a need to bring federal partners to their regular meetings – when possible – to provide a current level of awareness of the threat landscape.

   Root Cause Analysis

   Information is readily available to members of the transportation system sector however the participants didn't realize the vast number of resources out there nor who to tap to obtain that information.

Objective 2: *Met*

Assess how operators and stakeholders select, resource, share, and implement risk-based protective measures following a cybersecurity threat.

Objective Summary

Participants discussed how they obtain information from federal, state, local partners pertaining to known/unknown threats in their respective geographical area and in the bus industry. Additional conversation on considerations for sharing information with likeminded partners in their respective geographical area.

STRENGTH

1. **Best Practice:** Participants identified they have either internal or a 3rd party resource able to help them with cybersecurity issues when it directly impacts them. They also require all employees to take internal cybersecurity training should an incident occur.

AREA FOR IMPROVEMENT

1. **Area For Improvement:** While they do have policies, procedures and systems in place, participants identified they don't actively engage with their IT department or 3 party resource for identification of what has occurred in other parts of the transportation sector. They identified they aren't fully using all the resources offered by the federal government to include TSA and CISA.

   Root Cause Analysis

   Resources and services are readily available, and participants identified their organization can become overwhelmed by other situations thus making them susceptible to a cybersecurity incident.

Objective 3: *Met*

discuss physical and cybersecurity measures currently in place to protect the industry; identify wants, needs and desires.

Objective Summary

Participants discussed the relationship between the physical and cybersecurity relationship and the importance in identifying critical pieces when handling an incident. They discussed additional measures need to be applied should an incident actually occur considering the possibilities of back door interfacing from the buses to headquarters.

STRENGTH

1. **Best Practice:** Participants identified they are actively using their immediate resources to handle and mitigate cybersecurity threats. The usage of internal or 3rd party IT has proven to be the most beneficial aspect; however, they continue to feel that there is insufficient information being shared due to sensitivity considerations.

AREA FOR IMPROVEMENT

1. **Area For Improvement:** The need to establish a physical understanding when a cybersecurity incident occurs is important. It was identified in the event of a cybersecurity incident multiple systems could be impacted thus creating a physical demand as organizations would return back to paper copies and potential for issues from paying drivers to scheduling and tracking when present a critical failure within the organization. Historical information – paper copies – has not been dusted off or refreshed as everything is on computer system but the need to create redundancies in the system has proven relevant.

   Root Cause Analysis
   Historical/Paper copy management is not being taught or refreshed and unless an organization has tenured people there is a possibility for issues from paying personnel to schedule management.

Objective 4: *Met*

Discuss how transportation operators, stakeholders, and federal agencies can coordinate and communicate following a coordinated cyberattack

Objective Summary

Discussion on how information is shared among stakeholders with other stakeholders; with federal, state and local partners as well as sub operators within their organization(s) when looking at mitigating, responding and recovering from a cybersecurity incident.

STRENGTH

1. **Strength:** A select few participants identified times they have reached out to other organizations or federal partners to obtain additional information and/or asked their respective IT department or 3rd party entity to obtain additional information to cybersecurity attacks.

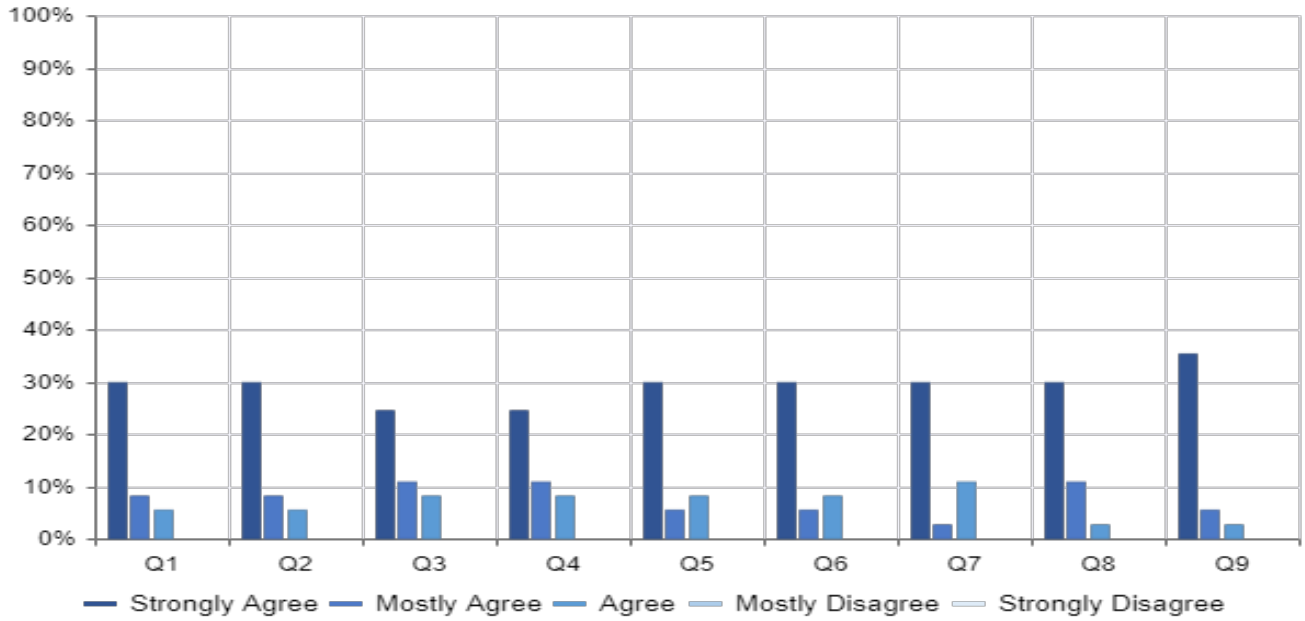
AREA FOR IMPROVEMENT

1. **Area For Improvement:** Multiple organizations didn't know all the offerings from federal partners and requested additional information to raise their cybersecurity baseline. Certain participants stated they wouldn't know who to call in the event of an incident beyond their insurance company and respective IT support (3rd party or internal) to help remedy the situation. One organization identified their leadership team wears multiple hats so their only solution is external support, and it would be focused on the response phase to get back up and running compared to preemptive or sustainment.

Participant Feedback

Overview

All participants had the opportunity to complete feedback forms, which allowed personnel to provide input on the content and conduct of the exercise. This section includes participants' feedback on the exercise and changes participants would like to implement within their organizations.



Feedback Questions:
Q1: The exercise was well-structured and organized.
Q2: The exercise scenario was plausible and realistic.
Q3: Participation in the exercise was appropriate for someone in my position.
Q4: Participants included the right people in terms of level and mix of disciplines.
Q5: The exercise was relevant to the risks facing my organization.
Q6: This exercise introduced new capabilities, resources, and information sharing that will enhance my organization's behaviors and preparedness.
Q7: The exercise afforded me the opportunity to network with federal, state, local, tribal, and/or industry stakeholders with whom I did not previously have established relationships.
Q8: The exercise was valuable to myself and/or my organization.
Q9: I would participate in an I-STEP exercise again.

Q10: Of what you learned today, what changes or improvements would you like to implement within your organization?

- Visa visit
- Ongoing education
- Cybersecurity
- Need to do a doomsday practice
- Can we have a paper back up
- Communication between IT and operations for a contingency plan if there is a major issue.
- Doomsday
- Putting a backup plan in place
- More awareness
- Backup systems to support our business continuity
- Better computer security
- SETA and TSTART to begin with

Q11: How do you think the exercise results will assist you in your risk-reduction efforts?

- Review policies and implement actionable items
- Extra caution
- Review of our cyber policies
- Will have greater conversations with IT
- More aware of risk
- A lot of helpful information that will be useful.
- Make sure everyone is aware of the risk.
- Made me think about a table top exercise
- Training
- It gives me ammo to get participation from my organization

Q12: Please comment on any ways future exercises could be improved.

- Need more exercises very thought provoking
- Discuss real life experiences of cyber intrusions
- More often
- Pace was rather fast. Many acronyms, but that comes with the territory lol

Q13: Please enter additional comments or feedback.

- Great job
- Appreciate the opportunity and education
- Thanks
- Well do this again
- Very impressive.
- Great collaboration
- Great collaboration and info sharing between industry partners

Full Scenario

Prevention

- Module 1:
  Media reporting continues to show a steady rise in Domestic Violent Extremists (DVE) and Homegrown Violent Extremists (HVE) using multiple social media platforms (Meta/Facebook, Instagram, Snapchat, TikTok, and Reddit) to express their opinions of the geopolitical climate. Additional reports continue to show potential cyberattacks against the bus industry with the intent to cause/create mass disruptions in their business operations.

  Update:
  FBI and CISA along with TSA and other federal agencies within the transportation community released multiple bulletins pertaining to cybersecurity threats against the Transportation system and advised organizations to take proactive measures to protect their organization.

Protection
Response

- Module 2:
  Your company begin receiving emails promising disruptions in communications, tracking system, ticketing system, billing system, and vital records management.
  One of your employees opens what they believe to be an official email, after clicking the provided link, they realized your company's name is misspelled in the subject line.

  Update:
  Your IT confirms multiple systems attacked: dispatching software, ticketing system, billing & invoices; driver communications, and ELD. Unknown how long the worm has been in the system and how deep the worm gained access.

  Update:
  (OPTIONAL): Your IT department has taken everything offline and projected 3-5 business days downtime – unless additional resources are needed – until return of normal operation.

Recovery

- Module 3:
  Attack impacts are known. Information sharing, reporting, and recovery processes enacted by the bus industry, LE and federal partners to return to service and operations.

Acronyms

Acronym	Definition
AAR	After Action Report
CIKR	Critical Infrastructure and Key Resources
COOP	Continuity of Operations
DHS	Department of Homeland Security
EXIS	Exercise Information System
FBI	Federal Bureau of Investigation
FSE	Full Scale Exercise
HSEEP	Homeland Security Exercise and Evaluation Program
HSIN	Homeland Security Information Network
ICS	Incident Command System
IED	Improvised Explosive Device
I-STEP	Intermodal Security Training and Exercise Program
JIC	Joint Information Center
JIS	Joint Information System
JTTF	Joint Terrorism Task Force
MOA	Memorandum of Agreement
MOU	Memorandum of Understanding
NIMS	National Incident Management System
NIPP	National Infrastructure Protection Plan
NTAS	National Terrorism Advisory System
OHSEM	Office of Homeland Security and Emergency Management
PIO	Public Information Officer
PP&E	Office of Policy Plans and Engagement

Acronym	Definition
SCAN	Surface Compliance Analysis Network
SME	Subject Matter Expert
SO	Security Operations
SOP	Standard Operating Procedure
SSI	Sensitive Security Information
TSA	Transportation Security Administration
TSOC	Transportation Security Operations Center
TSSSP	Transportation Systems Sector-Specific Plans
TTX	Tabletop Exercise
UC	Unified Command
WMD	Weapon of Mass Destruction