APTA STANDARDS DEVELOPMENT PROGRAM
RECOMMENDED PRACTICE
American Public Transportation Association
1300 I Street, NW, Suite 1200 East, Washington, DC 20006

APTA SS-ECS-RP-002-19
Published: March 27, 2019

Enterprise Cyber Security Working Group

Enterprise Cybersecurity Training and Awareness

Abstract: This document provides necessary information that transit agencies can use to begin building cybersecurity training and awareness programs.

Keywords: cybersecurity, training

Summary: This *Recommended Practice* helps people concerned about cyber-risks gain executive support to address cybersecurity risks via training and awareness programs. This *Recommended Practice* provides information to begin building an effective cybersecurity training and awareness program for an agency and has an associated PowerPoint document that can be used as the basis for a presentation to transit agency management.

Scope and purpose: The purpose of this document and its associated presentation are to help transit agency personnel develop and elicit support for a basic cybersecurity training and awareness program. This document may be amended with additional ideas for an effective program. Please send your feedback to APTA's Enterprise Cybersecurity Working Group.

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

© 2019 NATSA and its parent organization. No part of this publication may be reproduced in any form, in an electronic retrieval system or otherwise, without the prior written permission of NATSA.

Table of Contents

List of Figures and Tables

Participants

The American Public Transportation Association greatly appreciates the contributions of the **Enterprise Cyber Security Working Group**, which provided the primary effort in the drafting of this document.

At the time this standard was completed, the working group included the following members:

Leigh Weber, Cybersecurity Analysis, *Chair*

Lee Allen, *Transportation Security Administration*
Peter Anderson, *Greater Cleveland RTA*
DeLois Babiker, *Intellectual Concepts*
Antwan Banks, *MARTA*
Alesia Cain, *Hampton Roads Transit*
Rachel Deen, *Transit Safety & Security Solutions*
Barry Einsig, *Cisco Systems*
Sheri Ricardo, *Regional Transportation District*
Donald Luey, *Foothill Transit*
Daniel Miller, *TriMet*
David Teumim, *Teumim Technical*
William Tsuei, *Access Services*

Project team

Polly Hanson, *American Public Transportation Association*

Introduction

This introduction is not part of APTA SS-ECS-RP-002-19, "Enterprise Cybersecurity Training and Awareness."

APTA recommends the use of this document by:

- individuals or organizations that operate transit systems;
- individuals or organizations that contract with others for the operation of transit systems; and
- individuals or organizations that influence how transit systems are operated (including but not limited to consultants, designers, and contractors).

Note on alternate practices

Individual transit systems may modify the practices in this standard to accommodate their specific equipment and mode of operation. APTA recognizes that some transit systems may have unique operating environments that make strict compliance with every provision of this standard impossible. As a result, certain transit systems may need to implement the standards and practices herein in ways that are more or less restrictive than this document prescribes. A transit system may develop alternates to APTA standards so long as the alternates are based on a safe operating history and are described and documented in the system's safety program plan (or another document that is referenced in the system safety program plan).

Documentation of other practices shall:

- identify the specific APTA transit safety standard requirements that cannot be met;
- state why each of these requirements cannot be met;
- describe the alternate methods used; and

- describe and substantiate how the alternate methods do not compromise safety and provide a level of safety equivalent to the practices in the APTA safety standard (operating histories or hazard analysis findings may be used to substantiate this claim).

Enterprise Cybersecurity Training and Awareness

1. Why cybersecurity risk training and awareness?

Cyber-risks are introduced via technology; however, the solution is not solely technological. Instead, people are an essential part of the solution. They need to know how to identify cyber-threats and what to do about them. That concept is encapsulated in the well-known phrase "If you see something, say something."

Agency staff, contractors and partners, are all an essential part of cybersecurity because the vast majority of cyber-attacks begin when an untrained person inadvertently gives access to an attacker. Attackers use many ploys to entice or trick a person into granting the attacker access. The purpose of an effective training and awareness program is to help staff, contractors and passengers recognize these tricks and enticements. Training helps people understand the importance of reacting, how to react and to whom they should react.

1.1 What is at risk?

Transit agencies use information technology (IT) and operations technology (OT) in most, if not all, aspects of providing transportation to the public. Examples include accounting, human resources services, scheduling, communicating with the public, ticket vending machines, fare collection, vehicle location, vehicle repair and maintenance, telephones, emergency services, security cameras, and public information displays. As IT and OT become more integrated within a transit agency, a disruption to either will disrupt transportation service delivery and damage the agency's reputation.

A cyber-attack may damage the transit agency's reputation, resulting in:

- a decrease in ridership;
- an inability to get funding (loss of political support, inability to pass a bond referendum); or
- difficulty attracting and retaining a talented workforce.

2. Critical factors for a training and awareness program

These are the critical success factors for a viable cybersecurity training and awareness program:

- **Saying something:** This is measured by an increase in reports of suspicious activities, emails, requests for information, etc.
- **Discussion:** During all activities, the staff remains aware and concerned that information and routine operations are at risk from cyber-attack.
- **Action:** The agency can analyze and react to "saying something." If the agency is unwilling to take action, that will undermine the training and awareness program.

3. Authorization for a training and awareness program

The transit agency's executive management is busy juggling the many demands of providing safe and reliable public transportation while planning and providing for the future. As many agencies have fewer resources (people, money) than needed, it is easy to understand how cybersecurity threats may be overlooked. It is also

© 2019 American Public Transportation Association

understandable that non-IT executives and board members may not be fully aware of the threat that cyber-attacks present to the operation and reputation of the transit agency.

This *Recommended Practice* provides an outline to help agencies prepare a presentation to ask for executive sponsorship to lay the foundation for an effective cybersecurity training and awareness program.

4. The cybersecurity funding presentation

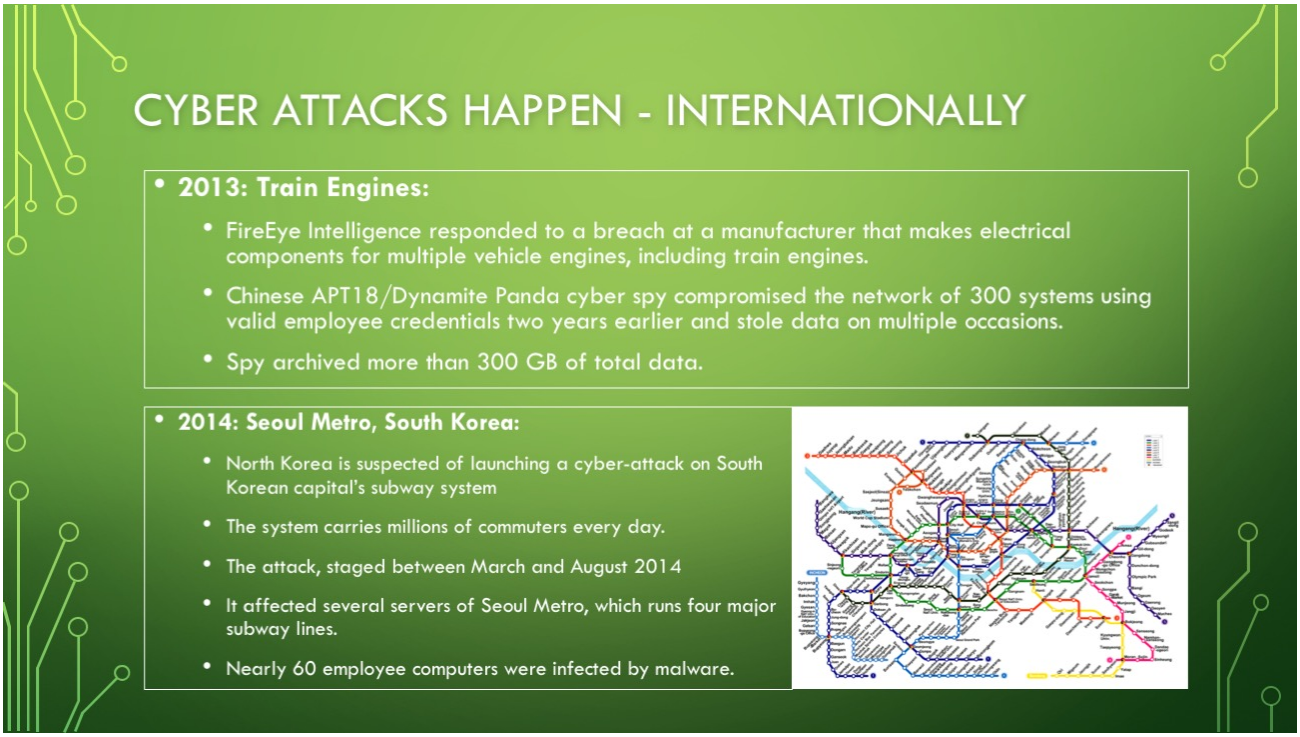
The PowerPoint presentation associated with this document represents the collective expertise and experience of the APTA Enterprise Cybersecurity Working Group. It and this *Recommended Practice* are designed to save agencies time.

> **NOTE:** Feedback about your experience with this presentation may be incorporated into future versions of this *Recommended Practice*. Please send all relevant feedback to APTA.

4.1 Presentation overview

Figure 1 shows a sample page of the PowerPoint presentation.

FIGURE 1
Presentation Example Page



The following are initial points to consider:

- **Who are you?** These materials should be used by the point person who wants to get a transit agency to launch a cybersecurity training and awareness program.
- **Who is your audience?** The audience for this presentation is the agency's executive management team (each agency uses different titles, but they may include president, CEO, general manager, executive director, etc.) or its board of directors.

© 2019 American Public Transportation Association

4.2 Presentation outline

4.2.1 Set the stage: Obtain executive buy-in

- We are here to show why the transit agency needs a viable cybersecurity training and awareness program and to take the steps necessary to establish a program that is sponsored by the highest authority of the transit agency.

4.2.2 Educate: Why is training necessary?

- Agency staff are busy doing their jobs; they are neither cybersecurity experts nor focused on cyber-scams.
- Show the audience what a cyber-attack/scam looks like.
- Teach the audience that it is OK to expect colleagues to follow the rules, such as always having photo ID displayed.
- Explain how to get employees to trust their sense of the normal and challenge the unexpected.

4.2.3 Educate: Cybersecurity training program drivers and plan deliverables

- Explain how the executive management team must hold the entire agency responsible and accountable for the success of the training program.
- Set the expectation of what the training plan will look like, including the level of detail that will be presented, time frames, initial cost, proposed scope or target population(s) of employees to train, people needed to contribute their knowledge and time, the nature of "outside" help needed, etc.
- Describe how you will measure and report on the effectiveness of the training program, either regarding employee participation, changes in observable behaviors, or both.

4.2.4 Implement: Ask for sponsorship to create the plan

- Ask for time, money and expertise to create the training and awareness plan. Expertise will be current transit agency staff, contractors, partners, and some external experts.
- Ensure that you have allies within your agency – once you have an executive sponsor, you need to ensure that your internal departments will support the efforts:
    - The department that does the training
    - HR
    - The physical security team
- Identify a specific executive or board member who will sponsor, and be accountable for, the effort.
- Identify the person who will run the project on a day-to-day basis and periodically report to the executive sponsor.

4.2.5 Next steps

- Draft the team members and the date to convene the first meeting.
- Set the first date to update the executive sponsor.

4.3 How to use the presentation

The PowerPoint presentation associated with this *Recommended Practice* contains slides that include material to present, as well as speaker notes. There are optional slides marked as "hidden." The "hidden" slides are additional materials that may be useful for your transit agency.

© 2019 American Public Transportation Association

It's important to stay focused on having a successful dialog with the audience. The goals are to get an executive sponsor and permission to create the plan, using the provided materials to help achieve the goal. To that end, each agency should make the presentation its own:

- Reorder the slides to match your presentation style.
- Select those slides relevant to your transit agency's situation—i.e., don't discuss rail issues for a bus-only agency.
- Update the slides with local and newer cybersecurity-related materials.
    - Ask your local FBI, TSA or DHS office for information.
    - Ask peer agencies for assistance and information.
- Do a practice session or two to ensure that your presentation achieves its goals.
    - Remember that executives often prefer brief, concise presentations.

4.4 Presentation tips

It's important to consider whom you are presenting to.

4.4.1 Board of directors

- Make the presentation *very short*—they either fund you, or they don't.
    - The assumption is that if the board of directors has put this presentation on the agenda, then they are ready to decide whether or not to fund the cybersecurity training program's roadmap.
    - If the assumption is incorrect and you need to educate the directors, then use a more extended presentation that explains the current risks and how to get started.

4.4.2 Executive management team

- If the executive team asks for a "deep dive," then prepare a longer presentation.
    - Educate your management.
    - Define the value of having a program and the time needed to "do it right" from the beginning.
- If informal approval has been given, and this presentation is only to get formal approval, then make it very short and to the point. Often just two slides are sufficient to formalize approval.

4.5 Presentation follow-up

After the presentation:

- Questions and answers—answer as well as you can
- Confirm the next steps:
    - Set a specific date for the next update/approval/action.
    - Assign responsibility to one person-in-charge to get the plan defined.
    - Identify specific people in the organization who will work on the team.
    - Identify a person to be the "champion" who can remove obstacles to ensure success.

© 2019 American Public Transportation Association

References

American Public Transportation Association Cybersecurity Materials:

[Enterprise] Cybersecurity Considerations for Public Transportation. http://www.apta.com/resources/standards/Documents/APTA SS-ECS-RP-001-14 RP.pdf

Securing Control and Communications Systems in Transit Environments, Part I: Elements, Organization, and Risk Assessment/Management. http://www.apta.com/resources/standards/Documents/APTA-SS-CCS-RP-001-10.pdf

Securing Control and Communications Systems in Transit Environments, Part II: Defining a Security Zone Architecture for Rail Transit and Protecting Critical Zones. http://www.apta.com/resources/standards/Documents/APTA-SS-CCS-RP-002-13.pdf

National Institute of Standards and Technology, "Framework for Improving Critical Infrastructure Cybersecurity." https://www.nist.gov/cyberframework

Transportation System Sector Cyber Working Group (TSSCWG): CyberSecurity@tsa.dhs.gov

Public Transportation Information Sharing and Analysis Center (ISAC): st-isac@surfacetransportationisac.org

Abbreviations and acronyms

DHS Department of Homeland Security
FBI Federal Bureau of Investigation
IT information technology
NATSA North American Transportation Services Association
NIST National Institute of Standards and Technology
OT operations technology (often SCADA or automation)
TSA Transportation Security Administration

Summary of document changes

- None

Document history

Document Version	Working Group Vote	Public Comment/ Technical Oversight	CEO Approval	Policy & Planning Approval	Publish Date
First published	Jul 18, 2018	Dec. 1, 2018	Jan. 8, 2019	Feb. 7, 2019	Mar. 27, 2019
First revision	—	—	—	—	—
Second revision	—	—	—	—	—

© 2019 American Public Transportation Association

Appendix A

PowerPoint Presentation Template: ECSWG_Training-2017-12.pptx

© 2019 American Public Transportation Association