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

APTA SS-ECS-RP-003-19
Published: March 27, 2019

Enterprise Cybersecurity Working Group

Enterprise Cybersecurity: Involving the Board of Directors and the Executive Suite

Abstract: This *Recommended Practice* is designed to help transit agency employees gain executive support for a basic cybersecurity program.

Keywords: cybersecurity

Summary: This *Recommended Practice* contains information and an associated presentation to help transit agency employees gain executive support for a program addressing cybersecurity risks. It provides information to share with executive management and the board of directors about cybersecurity threats to public transportation. The intended outcome is to obtain executive sponsorship and accountability for cybersecurity risk identification and mitigation.

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

Table of Contents

Participants

The American Public Transportation Association greatly appreciates the contributions of the **Enterprise Cybersecurity 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*
Michael Bosché Sr., *OCTA*
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-003-19, "Enterprise Cybersecurity: Involving the Board of Directors and the Executive Suite."

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: Involving the Board of Directors and the Executive Suite

1. Why cybersecurity risk management?

Transit agencies use information technology (IT) and operations technology (OT) in most, if not all, aspects of providing transportation to the public. They are used in, for example, accounting, human resources, scheduling, communicating with the public, ticket vending machines, fare collection, vehicle location, vehicle repair and maintenance, telephones, emergency services, security cameras, public information displays, and so on. As IT and OT become more integrated within a transit agency, a disruption to IT or OT will disrupt transportation service delivery.

In the most benign cases, an error made by IT staff, an IT supplier or an IT contractor can disrupt transit operations. In the most severe cases, a transit agency can be the intended target of a cyber-attack. Regardless of the cause of an IT/OT outage, the transit agency needs to be prepared to identify the problem, respond and then restore normal operations to continue providing safe, reliable transportation to the public.

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

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

2. Success factors for a cybersecurity program

These are the critical success factors for a viable transit agency cybersecurity program:

- **Accountable:** The most senior executive must be accountable for identifying and neutralizing cybersecurity risks. Being accountable does not mean the executive does the work; the executive will appoint others who are responsible for doing the detailed work. The executive must hold the responsible staff and contractors accountable on a regular basis to ensure that cybersecurity risks are routinely identified and addressed.
- **Ongoing:** The program must not just "check the box" to give the illusion that cybersecurity risks are being neutralized. Cyber-threats are evolving, and therefore as the threat likelihood and impact changes, the transit agency must regularly assess if it can withstand an attack and continue to provide transportation services safely and effectively.
- **Integrated with physical security:** Over time, cyber-threats will become just one method of threatening the overall security of a transit agency. Both cyber-threats and physical security threats need to be integrated into an overall security program.
- **Inclusive:** Although cyber risks are enabled by technology, the solution is not purely technological. People's awareness of cyber-threats and how to identify and address them are crucial to keeping cybersecurity risks in check.

- **Flexible:** Cyber-threats are ever evolving. Tested and true protection that worked yesterday may not work today. Transit agencies must ensure that their response plans are flexible enough to detect and neutralize the threat promptly.
- **Meaningful:** The program must generate meaningful value for the agency. Transit agencies should tailor the cybersecurity program to support their agency vision, mission, values, and requirements such that the program not only remains relevant but is aligned with agency-level priorities.

3. How to involve senior management

The transit agency's executive management is busy juggling the many demands of providing safe and reliable public transportation while at the same time 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 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 transit agencies prepare a presentation to ask for executive sponsorship to lay the foundation for an effective cybersecurity program.

4. The cybersecurity funding presentation

The PowerPoint presentation associated with this document (see Appendix A) 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 Using this presentation

The following are initial points to consider:

- **Who are you?** These materials should be used by the point person who wants to establish an effective cybersecurity 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.

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 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 a cybersecurity program 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.
- Show the history of cyber attacks that affected public transportation
- Explain the current set of threats as discussed by APTA, TSA, DHS, and other sources
- Explain the many IT and OT systems used by the transit agency and its contractors, then, some examples of what happens if a cyber attack compromises those systems

- Describe the costs associated with fixing a cyber attack after it occurs

4.2.3 Educate: Cybersecurity program drivers and plan deliverables

- Explain how the executive management team must hold the entire cybersecurity program to be responsible and accountable for its success.
- Set the expectation of what the cybersecurity plan will look like, (see Figure 1) including the level of detail that will be presented, time frames, initial cost, people needed to contribute their knowledge and time, the nature of "outside" help needed, etc.

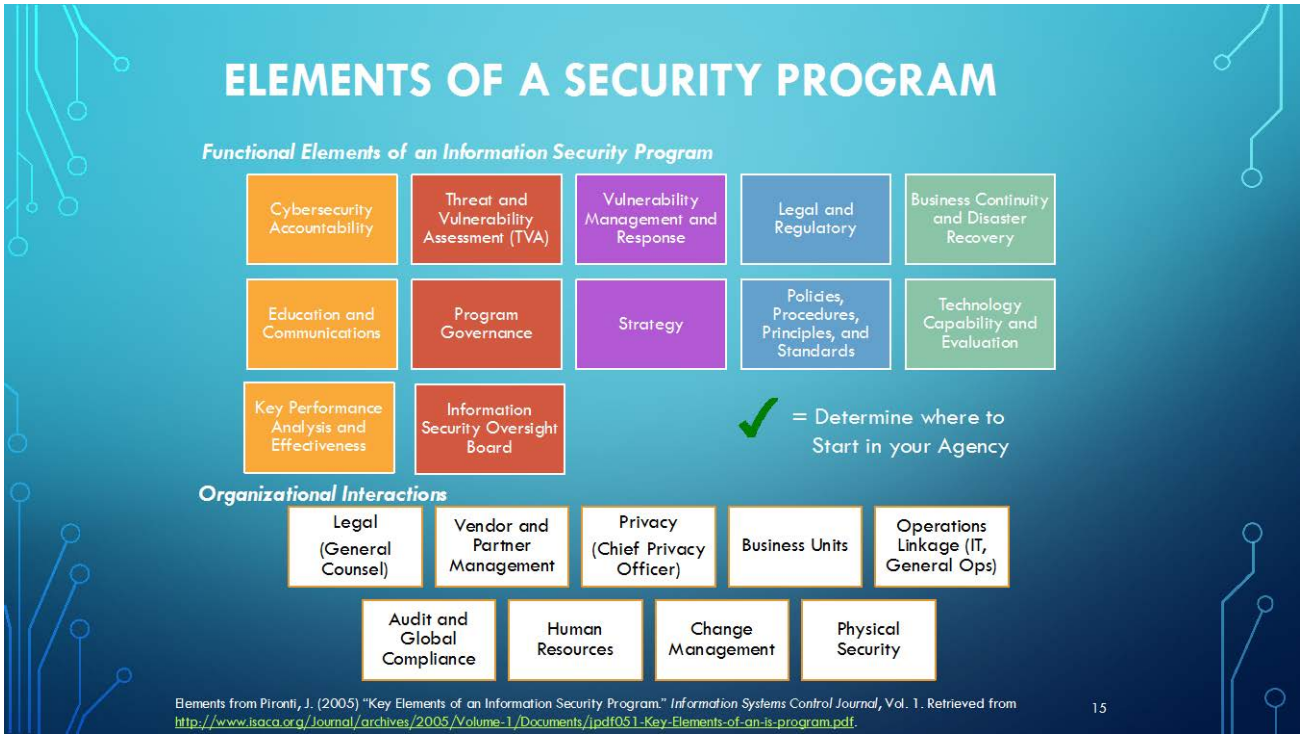

Figure 1 - Elements of a cybersecurity program

4.2.4 Implement: Ask for sponsorship to create a plan for the cybersecurity program

- Ask for time, money and expertise to create the cybersecurity program. Expertise will draw from current transit agency staff, contractors, partners, and some external experts.
- Ensure that you have lined-up some support within your organization before the presentation. Once you get permission to create a program formally, it helps to have allies. Try to find people who are also interested in cyber risk management from these departments:
    - HR/Training department
    - Finance/Accounting
    - Physical Security
    - IT department
    - Automation engineers, if applicable
    - Operations
    - Audit/Risk committee, if applicable

- Identify a specific executive or board member who will sponsor, and be accountable for, the effort. The best choices are the CEO/Managing Director/President, or Chief Operating Officer. Among the duties:
    - Help get resources
    - Ensure that various departments cooperate with 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.

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

- Focus on *fostering confidence* among the members of the Board that your program is beneficial, realistic, and will be well-managed.
- 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 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.
- Make sure that you do not surprise your Executive Management team.
    - It is essential that you have, at the very least, briefed your Executive Management before you present to your Board of Directors.

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.

References

Cybersecurity Considerations for Public Transit, APTA SS-ECS-RP-001-14
Overall Cybersecurity Handbook, NIST, 1995-October
Generally Accepted Principles and Practices for Security IT Systems, NIST, 1996-September
Managing Information Security Risk, NIST, 2011-March

Definitions

xx

Abbreviations and acronyms

DHS Department of Homeland Security
ECSWG Enterprise Cybersecurity Working Group
FBI Federal Bureau of Investigation
IT information technology
OT operations technology (often SCADA or automation)
TSA Transportation Security Administration

Summary of document changes

Document history

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

Appendix A: PowerPoint presentation template

PowerPoint Presentation Template: ECSWG_InvolveExecutives-2018-06.pptx