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

APTA SS-ECS-RP-004-23
First Published: May 31, 2023

Enterprise Cyber Security Working Group

Developing a Cybersecurity Program That Meets an Agency's Needs

Abstract: This recommended practice provides planning tools to help transit agency security professionals address cybersecurity risks in a sustainable and effective way that aligns with the agency's vision and mission.

Keywords: cybersecurity, information security, risk management

Summary: Even the most seasoned security professional can't tackle all elements of developing a cybersecurity program single-handedly, nor will doing so in a vacuum result in an effective, well-rounded program. Help is required to acquire the managerial, financial and organizational support needed. A solid cybersecurity program is based on a well-informed strategy that aligns with an agency's wants and needs. This recommended practice provides strategic planning tools and principles to help security professionals understand the drivers for cybersecurity in an agency, see how those map to the agency's vision and mission, identify stakeholders in a cybersecurity program, and establish a steering committee of stakeholders to help develop an effective, well-supported and sustainable program.

Scope and purpose: This recommended practice is intended for use primarily by cybersecurity, information security and risk management practitioners or other individuals with cybersecurity or risk management responsibilities at small to medium-sized transit agencies. It is also designed to inform executives and senior managers who are helping to support such a program. The tools in this document will help security professionals identify an agency's cybersecurity wants and needs; understand the stakeholders who could best support the program's success; and identify an appropriate executive champion and develop a steering committee to help develop, refine and constantly reassess the program.

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 this 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.

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:

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

Terry Follmer, *CAP-Metro*
Michael Bosche, *Orange County Transportation Authority*
Lee Allen, *TSA*
Antwan Banks, *MARTA*
Donald Luey, *Foothill Transit*
Leigh Weber, *Cybersecurity Analysis, Ltd.*
Tim McHugh, *TriMet*
Peter Anderson, *GCRTA*
Christopher Martin, *TriMet*
Claire Mueting, *TSA*
William Tsuei, *Access Services*
Ryan Sean, *MTA Metro-North Railroad*
Tim Coogan, *Regional Transportation District*
Polly Hanson, *American Public Transportation Association*
Sheri Ricardo, *Regional Transportation District*
Alesia Cain, *Macro a Division of Ross & Baruzzini*
DeLois Babiker, *Intellectual Concepts*
Ahmed Idrees, *Sound Transit*
Julius Smith, *DART*
Jack Ren, *AC Transit*
Daniel Miller, *TriMet*
Chris Shepherd, *Gannet Fleming*
Jack Sherman, *Hampton Roads Transit*
Daniel Sullivan, *Regional Transportation District*
Jeff Vanwingerden, *Sound Transit*
Muneer Baig, *SysUSA*
Melivan Beard*, Regional Transportation District*
Rachel Deen, *Transit Safety & Security Solutions*

Introduction

This introduction is not part of APTA SS-ECS-RP-004-23, "Developing a Cybersecurity Program That Meets an Agency's Needs."

Applying this recommended practice will allow security personnel to do the following:

- Identify the agency's needs and wants relative to cybersecurity (business strategy).
- Understand who at the agency could best support and influence (or most challenge) the program's success (stakeholder analysis).
- Identify an appropriate executive champion for the program and develop a steering committee that will help the agency develop, refine and constantly reassess its cybersecurity program.

This recommended practice is intended for use primarily for cybersecurity, information security, risk management practitioners or other individuals with cybersecurity or risk management responsibilities at small to medium-sized transit agencies. It is also intended to inform executives, senior managers and department heads of the need for their participation and support to establish an ongoing rapport regarding the agency's cybersecurity strategy and needs.

Developing a Cybersecurity Program That Meets an Agency’s Needs

1. Understanding agency needs and wants

While there are many different approaches to creating a cybersecurity program, the most effective and sustainable programs are aligned with the agency’s overall vision and mission. When the cybersecurity program is strategically aligned with the agency, it is easy for managers, peers, customers, and cybersecurity staff to do the following:

- Envision cybersecurity as a contributor to concrete, visible, positive progress for the agency (vs. a competitor or enemy).
- Build a positive reputation for and maintain good morale among the cybersecurity staff and with other departments.
- Increase the level of risk sensitivity and awareness at every level, driving down unforeseen gaps and avoiding future issues.
- Position the program to attain the support (staffing, budget and priority) needed to further cybersecurity initiatives that make transit better and safer for all.

With a brand-new program, while the agency leadership may understand that there are cyber-threats to be addressed, it’s reasonable to consider that they may not have given much serious thought to where technology components exist in the agency, let alone which technology assets are the most important to secure or how to secure them. This requires that the lead security professional develop a solid understanding of what the agency has, wants and needs, and that others be brought to this same understanding.

1.1 Understanding an agency’s vision and mission

To understand what an agency is about, consider these important questions:

- What are the agency’s vision, mission and strategic plan? What is it interested in achieving generally? (Consider the agency’s website, strategic plan, annual goals, GM goals.)
- What major projects are being undertaken this year? In the next five years? (Consider build-out of system, renovation, integration with partners, etc.) Which of these involve technology, and how?
- Which groups or functional areas have the most interest or priority?
  - Consider groups that administer technology, both IT and outside IT (e.g., OT/SCADA, CAD, garages, vehicles)
  - Consider business groups such as safety, security, legal, etc.

Other resources for understanding an agency’s vision and mission:

- official vision/mission statements
- agency public website “Who We Are” or “About” pages
- agency internal website
- marketing materials, social media, branding

- key performance indicators (KPIs)
- board meeting notes, or attend a public board meeting
- general manager's goals
- agency strategic plan and roadmap (e.g., five-year plan)
- other departments' strategic plans
- agency-hosted training courses, working groups and committees
- interviews with management
- agency COOP

1.2 Understanding an agency's culture

To understand an agency's culture and how it operates, consider the following questions:

- How does the organization approach staffing? Does it like to run lean? Have a lot of staff? Like to contract or outsource? Have preferred partners for contracting?
- Does the organization interface much with other local or government agencies? What are the agencies' partners and existing relationships?
- Is the organization in a "growth" mind-set or a "sustain" mind-set? With regard to transit operations generally? With regard to IT?
- How easy or difficult is it to build and sustain relationships within the organization? How do people work together and accept direction? How do they communicate? What motivates them?
- How does the organization respond to the chain of command, or does it manage differently? Is the direction from the top clear, or is it driven from the bottom?

Resources for understanding the agency's culture:

- policies and procedures
- communications style (formal, informal)
- communications vehicles such as websites, newsletters, email, text/phone, Slack,webinars, interoffice mail
- chain of command
- staff interviews

1.3 The challenge: What if nobody cares?

One important note about culture: Culture eats strategy for breakfast (and policy for lunch). Applying a cybersecurity strategy in a very risk-tolerant culture requires that security professionals find ways to work with the culture, or that they try to change the culture.

2. Understanding the business climate

The PEST (Political, Economic, Social and Technological) tool is useful for developing a well-rounded understanding of the external forces acting upon an agency—whether they are directly related to cybersecurity or not. Typically these forces are beyond security professionals' control, but understanding them can help identify areas of risk and opportunity, articulate cyber-risks associated with these forces, and understand how cybersecurity can support agency goals.

To apply PEST, think about how political, economic, social and technological external forces influence an agency's continued operational success. Equal analysis should be applied to each factor. The results can be visualized on a grid.

A sample grid with examples of PEST categories that might be relevant to a transit agency is pictured in **Table 1**. Caution: Each agency has different challenges. **Table 1** is provided as a prompt to motivate thinking about an agency's current position relative to these areas to identify possible risks and opportunities.

TABLE 1
PEST Categories

Political	Economic
• Laws and regulations • Political relationships (e.g., with the city, state) • Public vote (e.g., publicly elected board or transit proposals)	• Ridership statistics (up/down/steady) • Interest and income rates • Spending or procurement policies • Vendor relationships
Social	**Technological**
• Customer or employee lifestyles and attitudes • Workforce availability • Customer demographics • Population shifts	• Technology life span (ability to replace or update) • Control systems • Availability of new technology (e.g., self-driving vehicles, connected devices)

2.1 Cybersecurity threat analysis

Understand what assets at the agency are the most important to protect: What are the agency's "crown jewels"? Knowing which, whether and how any of these crown jewels intersect with technology will help with a more specific threat analysis.

These are the important questions to ask:

- What prompted the need for or interest in cybersecurity at the agency (general interest, public inquiry, board interest, IT expressed need, incidents, etc.)?
  - Has a risk assessment been performed? By whom, when and on what areas? What most concerned the agency? Who was most concerned?
  - Has a direction or specific need been expressed (e.g., monitoring, training, risk management, information security, all of the above, nothing specific)? By whom?
- Does the agency have any compliance needs or concerns (e.g., GDPR/protection of PII, PCI, HIPAA or SSI)?

Resources for understanding cyber-risks to the agency:

- government or private threat intelligence reports (e.g., by TSA or ISACs)
- industry risk reports (e.g., Verizon DBIR or others)
- published exploits, including those that are technical and those that are "news"
- high-level risk surveys (e.g., insurance surveys, CSET)

Not all agencies have a concrete idea of their threats and vulnerabilities, so the other analysis tools will be more useful in gaining a general understanding of the agency's threat climate until such a basis is developed.

2.2 Additional tips

Some final thoughts and key takeaways on strategic analysis:

- Do not rely on "official sources" only; diversify. Obtain a well-rounded picture of the agency's needs, wants and people.

- Do not look only for or at technology or IT-related materials. Understand how the agency works as a whole, even the parts that don't use computers.
- Consider what public face or image the agency portrays and what feeling it gives.
- Go out into the world: Meet others face to face and ask them what they do. Tour other facilities. Don't stay behind the computer.
- Take notes so the lessons learned can be applied when developing a steering committee and, later on, a program roadmap.

3. Understanding stakeholders

In addition to understanding the agency's vision, culture and threats, it's important to understand what specific people (individuals or groups) at the agency are decision-makers and influencers who will contribute to or challenge a cybersecurity program's success. Performing stakeholder analysis will help to identify who they are, what motivates them, what interests them about the program, and their ability to influence the program. This analysis will also help security professionals to choose wisely when soliciting participants for the program's steering committee.

3.1 Identifying stakeholders

The analysis of the agency's vision, mission and culture probably produced some idea of who the program stakeholders might be, but it is best to do a little more structured analysis.

A useful tool for identifying stakeholders is SIPOC, which stands for suppliers, inputs, processes, outputs and customers. This is a five-step methodology for identifying stakeholders who contribute inputs to, or consume outputs of, a business process. The steps are to identify the following:

1. the process (parts)
2. process outputs
3. consumers of those outputs (customers)
4. prerequisites for the process (inputs)
5. who supplies those inputs

For first-time program development, security professionals should consider speculating on what they think they might need or produce from the cybersecurity program at a very high level, and who would supply or consume those inputs or outputs. The full SIPOC method can be used again as cybersecurity projects and initiatives are developed and the processes and players change.

Similar to the PEST method, the results of SIPOC can be mapped to a grid. An example of a modified SIPOC analysis for a new cybersecurity program is shown in **Table 2**. Caution: Each agency is different; the groups and individuals identified as stakeholders should map to the agency's own organizational structure and what was learned through the research on its strategic priorities and culture. The inputs and outputs may vary based on how the agency delegates authority, divides resources, addresses tasks and consumes information.

TABLE 2
Sample SIPOC Analysis

Suppliers	Inputs (Needs)	Process	Outputs (Products)	Customers
• CFO (budget) • CIO (IT manager) • Materials management (procurement of goods and services) • CSO (safety/security) • Vendor partners (e.g., MSSP)	• Funding • System admins • RFP/supplier management • Managerial authority • Staff with specific skills	• The cybersecurity program	• Policies and procedures • Compliance reports (gap analysis) • Trend or progress reports • Risk register	• Computer users (multiple departments) • Computer administrators (IT) • Operations teams (control systems) • Auditors • GM/board of directors

3.2 Getting to know stakeholders

Once a pool of prospective stakeholders has been identified, it's important to meet with each of them to understand their perspectives (if not already done during the earlier research). Consider the following questions:

- What motivates them?
- What do they want or need from the program or the security professional?
- What are they most interested in, related to the program or related to the agency?
- What could the program contribute to them?
- What is their relationship with others within the agency (e.g., trusted staff or allies)?

Most transit agencies are people-focused organizations. Despite the existence of conferencing technologies, if it is at all feasible, it is imperative to meet stakeholders face to face, on their grounds. This will allow them to show the security professional what they are excited about, and provide an opportunity to learn, observe and think about how the cybersecurity program could contribute to that person or their department's goals—or benefit from their help.

4. Developing a steering committee

4.1 Soliciting an executive champion

Most practitioners in new cybersecurity programs "fall into" or are "assigned" the responsibility of developing a cybersecurity program, and some are brought in from the outside. They may already report to a specific department or arm of the organization (for example IT). Their existing report-to executive may be the best choice for an executive champion because of his or her level of interest and ability to push the goals of your program forward, but this is not always the case. Here are some things to consider when soliciting an executive champion:

- How might the program be funded? What resources could be needed, and who controls those resources?
- Who is likely to be affected by the actions of the new program? How and to what degree?
- Who has expressed interest in the program and why?
- How do things get reviewed and approved at the agency? Who is involved, and what is their role?
- Based on an analysis of the organization, how does cybersecurity best align with the agency's needs, priorities and organizational structure? For example, is the need for the cybersecurity program more skills and technology-focused (e.g., on system administration)? More safety or security-focused (on directing or assessing people, policy and operations)? Both? And to what degree?

Soliciting feedback from other organizations or researching organizational frameworks in white papers and publications can help frame the thinking around where the program is best situated within an agency's organizational structure—which may or may not influence the report-to chain—by looking at what has worked for others and generic strategic advantages and disadvantages. For example, ISACA's COBIT 5 for Information Security offers an analysis of different C-level reporting paths for information security. Similar to the suggested key questions above, this analysis considers, among other things, the C-level champion's degree of authority within the agency, ability to direct or influence changes (e.g., to technology, operations), primary mission and responsibilities, methods of digesting information, and degree of influence on the agency's roadmap (business or technological). It also offers a list of pros and cons of choosing certain C-suite champions.

Regardless of other available models and advice, the best place to position the program at an agency is the place where the security professional can (a) get the most support to grow the program and (b) have the most direct influence on the needs and wants that matter most to the agency so the program provides genuine value and is visible to others. As the agency's cybersecurity needs change, the security professional can make a pitch to change executive sponsors, but that is not easy to do once the program has been established. If the security professional is already aligned with an executive champion (via direct reporting or delegation), he or she may wish to use the questions and research proposed in this section and in Section 3 to assess the executive's position to and interest in the program, and ways in which he or she can best support it.

4.1.1 Developing the committee charter

The committee charter should do the following:

- Elaborate on the reason the committee exists in terms of its value and contribution to the agency's overall needs and wants.
- Identify the committee members, their roles and the importance of their roles on the committee.
- Set clear expectations for the committee members (i.e., identify what inputs they will give).
- Specify how the committee communicates (meetings, website, email, etc.) and how frequently.
- Identify outputs of the committee (what it hopes to achieve and what products it will manage). Among the first of these, the committee should address the program roadmap, including its development, refinement, and continual review and improvement.

5. Conclusion

The best cybersecurity program is one that "does something that means something." It is less important where the agency starts than that it starts somewhere. Whether in a structured or more organic way, the security program can grow to meet an agency's needs and priorities as it matures over time. Using the strategies in this document can help to leverage the agency's culture and resources (human, technology and best practices); maintain a reasonable workload; select a committee of individuals who can help navigate what the agency needs so that the program provides value; and continually assess and align the program with the agency.

References

Kim, Frank, Northcutt, Stephen, SANS Institute. (2017). MGT514: IT Security Strategic Planning, Policy, and Leadership: 514.1 Strategic Planning Foundations. Maryland, USA: SANS Institute.

ISACA. (2012). COBIT 5 for Information Security. Rolling Meadows, IL: ISACA.org.

Abbreviations and acronyms

CAD	computer-aided design
CFO	chief financial officer
CIO	chief information officer
COOP	Continuity of Operations Plan
COBIT	Control Objectives for Information and Related Technology
CSET	Cyber Security Evaluation Tool
CSO	chief security officer
DBIR	Data Breach Investigations Report
GDPR	General Data Protection Regulation
GM	general manager
HIPAA	Health Insurance Portability and Accountability Act
ISAC	information sharing and analysis center
ISACA	formerly the Information Systems Audit and Control Association
IT	information technology
KPI	key performance indicator
MSSP	managed security service provider
NATSA	North American Transportation Services Association
OT	operational technology
PCI	Payment Card Industry Data Security Standard
PEST	political, economic, social, technological
PII	Personal Identifiable Information
RFP	request for proposal
SCADA	Supervisory Control and Data Acquisition
SIPOC	suppliers, inputs, processes, outputs, customers
SSI	Sensitive Security Information
TSA	Transportation Security Administration

Document history

Document Version	Working Group Vote	Public Comment/ Technical Oversight	Rail CEO Approval	Policy & Planning Approval	Publish Date
First published	Jun 6, 2020	Mar. 31, 2022	May 9, 2022	June 22, 2022	May 31, 2023