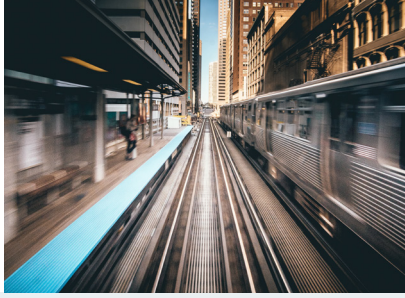
REPORT SUMMARY

FTA Report No. 0250
August 2023

FTA RESEARCH
FEDERAL TRANSIT ADMINISTRATION



CYBERSECURITY RESILIENCE ASSESSMENT TOOL TO ENHANCE PUBLIC CONFIDENCE IN TRANSIT

Background

Public transit agencies provide a vital service to the communities in which they operate. The talented teams of people running these operations are tasked not only with keeping services running in varied conditions, but also increasingly with finding ways to incorporate new technologies to augment and modernize everything from fare payment to scheduling management to back-office operations. As public entities, most agencies are working to integrate these technologies with razor thin margins and personnel who may have limited experience running technology-driven organizations.

Transit agencies are learning that with these new technologies comes increased risk, more specifically cyber risk. The global transportation sector experienced a 186% year-over-year increase in weekly ransomware attacks since June 2020, according to Check Point.[1]

For transit agencies at the beginning stages of incorporating cybersecurity practices into their organizations, there is no better place to start than with a cybersecurity self-assessment. The assessment process—like an audit or accounting—establishes a baseline of the agency's current safety, security, and risk operations and if/how cybersecurity best practices are included. People, processes, policies, partnerships, and technologies are all considered. The results of the assessment are not a judgment of the organization and its personnel, but often offer a wake-up call for agency leadership to make cybersecurity a priority.

For organizations that are new to managing interconnected, technology-dependent operating environments, the traditional cyber assessments and framework guides can be daunting and too advanced. When every assessment category comes back as "red" or "in need of immediate attention," it can be a challenge to know what to prioritize and where to start. In 2021, FTA recognized the need for a better cyber assessment on-ramp for public transit agencies. Via a grant to the Rock Island County Metropolitan Mass Transit District (MetroLINK) in Illinois, Max Cybersecurity and Grayline Group were engaged to design a cyber assessment tool to make integrating best cyber practices more accessible for public transit agencies.

Objectives

The objectives for the project were to:

- Develop a cybersecurity risk assessment framework customized for the public transit industry
- Develop a tool that assists public transit agencies in assessing their cybersecurity preparedness
- Use the tool to assess MetroLINK's cybersecurity preparedness and refine it based on the experience
- Promote adoption of the tool to transit agencies, and further engage government and private sector entities to enhance cyber risk preparedness at agencies

[1] https://blog.checkpoint.com/2021/06/14/ransomware-attacks-continue-to-surge-hitting-a-93-increase-year-over-year/

Findings and Conclusions

The final product of the reimagined cyber assessment is the Cybersecurity Assessment Tool for Transit (CATT)—a tool designed to help resource-constrained public transit agencies develop and strengthen their cybersecurity program to identify risks and prioritize activities to mitigate them.

The main features of CATT:

- Defines key words throughout the assessment so that individuals without cyber, IT, or detailed technical knowledge can more easily navigate the questions
- Provides statements to choose from that best describe the organization
- Provides a "green, yellow, red" read-out of each section to help prioritize next steps
- Includes a Cyber Resilience Review Supplemental Guide with transit-specific tools and resources noted for each domain to help the agency develop plans and implement practices to improve their operational resilience
- Includes operational technology and safety-related questions
- Aligns with National Institute of Standards and Technology Cybersecurity Framework which provides organizations with guidance on improving critical infrastructure cybersecurity

Benefits

Once an agency completes its first cyber assessment using CATT, the tool generates a report with the assessment findings prioritized to inform actionable next steps. At the early stages of improving operational resilience and cyber practices, the best practice is to complete the assessment at least once a year. CATT will help transit agencies improve their cyber posture and serve as a steppingstone to other tools and resources available.

Critical infrastructure must keep pace with the evolving threat landscape, and there is little doubt that this becomes increasingly complex as more points of access connecting machines and services to the Internet become the norm. Whether a public transit agency is just beginning its cybersecurity journey or is a few years in, CATT serves as an important resource for strengthening cyber practices, cyber literacy, and the ability to deliver agency services safely and reliably to their communities.

FTA Report No. 0250
Project Information

This research project was conducted by Max Cybersecurity and Grayline Group on behalf of MetroLINK. For more information, contact FTA Project Manager Raj Wagley at (202) 366-5386 or Raj.Wagley@dot.gov.

All FTA research reports can be found at https://www.transit.dot.gov/about/research-innovation.