SJSU SAN JOSÉ STATE UNIVERSITY

MTI MINETA TRANSPORTATION INSTITUTE

Aligning the Transit Industry and their Vendors in the Face of Increasing Cyber Risk: Recommendations for Identifying and Addressing Cybersecurity Challenges

Scott Belcher Kathryn Seckman Homayun Yaqub
Terri Belcher Brandon Thomas

Project 2113
July 2022

Introduction

U.S. Public Transit agencies are highly dependent on the services of vendors to help deliver and maintain critical technologies that are linked to everything they do from ticket purchases to email management. The vendor's cybersecurity posture (the strength of their controls and protocols)—whether immature or advanced—is shared with their clients. The U.S. transit industry and its vendor community have the opportunity to broaden their relationships and focus on cybersecurity. Both parties need to create a security environment that can benefit from and augment the other.

Study Methods

Research methods included oral interviews with key vendors of the public transit industry, transit operators, and other important stakeholders (e.g., members of the Executive Branch, Congress, other industries, and relevant trade associations) and an extensive review of literature published in periodicals and online.

Findings

The authors' findings focus on three key areas: cyber literacy and procurement practices, the lifecycle of technology vis-à-vis transit hardware, and the importance of embracing risk as a road to resiliency.

Transit agencies need to use the procurement process as an opportunity to articulate their cyber needs because the presence of such requirements in requests for proposals (RFPs), is a key driver of investment for vendors. Transit Agencies must also have a sense of their own risks and have the ability to communicate these risks in technical terms that align with the actual needs of the organization or service delivery being sought from the vendor.

Similarly, the authors underscore that the hardware and software lifecycles in public transit are out of sync, creating a situation in which vehicles and other hardware designed to last for 15 years or more are being supported by or carrying software that stopped receiving security updates

five years after it was launched. This disconnect creates serious vulnerabilities.

Multiple vendor interviews highlighted the importance of viewing organizational needs through lenses that focus on risk and security and how understanding the difference is fundamental for addressing cyber risks. A risk-focused mindset would not only help transit agencies in their own cyber risk management but also position them to gain more from their vendor relationships.

Policy/Practice Recommendations

There are several steps that transit agencies and their stakeholders can take to strengthen their collective cybersecurity posture. These measures require executive focus and investment across the transit ecosystem.

- **Vendors** for critical systems should make available a security lead to assist the agency in the management of the agency's risk. They should establish a cadence for periodic and independent security audits and penetration testing of their environments.
- **Transit Agencies** should integrate their cyber risk management program with their existing physical security risk management organization and infrastructure, creating a holistic Enterprise Risk Management program. They should also elevate security within the organization by appointing a Chief Security Officer (CSO).
- **Associations** should develop third-party risk management and oversight standards and incorporate them into templates for contract language, RFPs, and other artifacts that operators can rely on to engage the vendor community.
- **The Department of Homeland Security (DHS)** and U.S. Department of Transportation (U.S. DOT) should create a Sector Cybersecurity Executive with dedicated investment and authority to establish sector and subsector cybersecurity guidance.
- **The Federal Transit Administration (FTA)** should require all procurements using federal dollars include and fund basic security maintenance when software and firmware are procured and that all transit agencies meet the basic requirements set forth in Transportation Security Administration (TSA) Security Directive 1582-21-01.
- **Congress** should increase funding to DHS and U.S. DOT to develop a set of minimal cybersecurity standards and increase formula grant funding to transit agencies to ensure that they have the resources to meet the minimal cybersecurity standards established above.

About the Authors

Scott Belcher, JD, MPP
Scott Belcher is the President and CEO of SFB Consulting, LLC.

Kathryn Seckman, MA
Kathryn Seckman is the Executive Director of Strategy and Analysis at Grayline Group.

Terri Belcher
Terri Belcher is a writer and analyst who has worked in Washington, D.C. for 30 years.

Brandon Thomas, MBA
Brandon Thomas is a Partner at Grayline Group.

Homayun Yaqub, MA
Homayun Yaqub brings 25+ years of security and risk management experience, as a Global Security Strategist at Forcepoint and has lead risk and security initiatives at JPMorgan Chase.

To Learn More

For more details about the study, download the full report at **transweb.sjsu.edu/research/2113**

MTI is a University Transportation Center sponsored by the U.S. Department of Transportation's Office of the Assistant Secretary for Research and Technology and by Caltrans. The Institute is located within San José State University's Lucas Graduate School of Business.