SJSU SAN JOSÉ STATE UNIVERSITY

MTI MINETA TRANSPORTATION INSTITUTE

Does the Transit Industry Understand the Risks of Cybersecurity and are the Risks Being Appropriately Prioritized?

Scott Belcher, JD, MPP
Terri Belcher
James Grimes
Lusa Holmstrom
Andy Souders

Project 2405
April 2025

Introduction

In 2020, the Mineta Transportation Institute (MTI) published Is the Transit Industry Prepared for the Cyber Revolution? Policy Recommendations to Enhance Surface Transit Cyber Preparedness (2020 MTI Study). In that study, the authors reported that the transit industry was ill-prepared for cybersecurity threats and attacks. This study updates the 2020 MTI Study. After four years and the establishment of new cybersecurity requirements from the U.S. government as well as the availability of new and numerous free resources, the cybersecurity preparedness of transit has not markedly improved. In fact, this study shows that smaller transit agencies lag far behind their larger peers and are especially at risk.

The objective of cybersecurity is to protect the entire organization, encompassing both Information Technology (IT) and Operational Technology (OT) environments, from unauthorized access and malicious threats. The increasing sophistication of cybercriminals, in combination with a greater reliance on technology within the transit industry, puts the industry at higher risk than in 2020. A cybersecurity breach can impact the financial viability, operational capability, and reputation of the organization. Without action to strengthen cybersecurity preparedness significantly, the industry will continue to be at increased risk of cybersecurity attacks that potentially expose sensitive data, disrupt operations, and cause harm.

Study Methods

Research methods included an online survey, oral interviews with public surface transit agencies in the United States and key public and private sector representatives, and literature research. Altogether, the agencies that responded to the survey serve over 72 million people—roughly a fifth of the entire population of the United States. Of the 78 agencies, one third of respondents are considered rural, having lower population densities and different operating models.

This study provides a transit industry overview; reviews the transit cybersecurity risk profile; existing guidance for transit; and provides policy recommendations for

Congress, the Executive Branch, public surface transit agencies, and their associations and other supporting organizations.

Findings

The report has three major findings. First, there is a lack of organizational knowledge about cybersecurity. Many executives do not appreciate the cybersecurity risks their organizations face, and if they do, many leaders do not know what their teams are doing to address these risks. Second, many agencies lack important documented policies and procedures. The survey responses demonstrated a lack of documented policies and procedures across a broad spectrum of requirements that are considered essential by most cybersecurity professionals. Third, small agencies lag far behind large ones. For all of the best practices discussed in the report, a bigger proportion of the larger agencies adhered than did smaller agencies.

Of the agencies that responded, over a third said they were not performing annual cybersecurity assessments. Even more concerning, however, is the size of many of the agencies that reported never having completed a cybersecurity assessment. Among these nine agencies, four had operating budgets of more than $30 million in 2022, and one agency had over $100 million. These agencies are large enough to have the internal resources needed to complete a free cyber assessment. Additionally, while almost all agencies with operating budgets above $50 million employed at least one full time equivalent (FTE) for cybersecurity, less than half of the agencies in the smallest category did so.

Policy Recommendations

The authors made a number of policy recommendations intended to engage the U.S. Congress, the Executive Branch, transit agencies, associations, and other supporting organizations to find ways to establish a minimal set of cybersecurity requirements, provide funding to implement them, and inform agency leadership about the need for action. Recommendations for agencies include:

- Transit agencies should develop an individualized cybersecurity plan that takes advantage of the best practices identified above and update it at least annually.
- Transit agencies should conduct a cybersecurity assessment at least annually and address the shortcomings identified in that assessment in a timely manner.
- Transit agencies should ensure that they have documented cybersecurity policies and procedures in place and that the organization is following them.
- Transit agencies should ensure that they have at least one person on staff with a cybersecurity certificate and are qualified to oversee the overall cybersecurity program and/or cybersecurity vendors.

About the Lead Authors

Scott Belcher is a Research Associate with the Mineta Transportation Institute and has 35 years of experience in Washington, D.C. with the federal government as a lawyer and as an executive with several trade associations. Scott has spent the majority of his career working on transportation technology issues.

Andy Souders is a technology executive with over 35 years of experience in digital innovation and organizational transformation across industries such as Cloud, Cybersecurity, and Smart Cities.

To Learn More

For more details about the study, download the full report at transweb.sjsu.edu/research/2405

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.