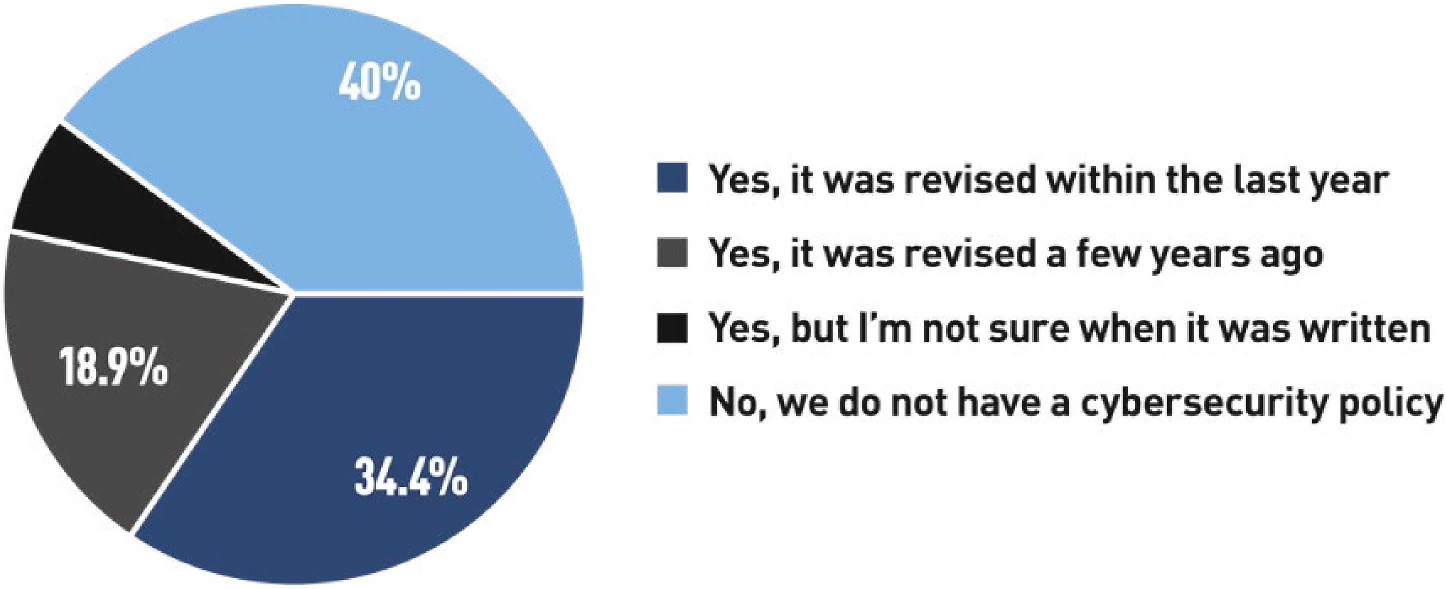
SJSU SAN JOSÉ STATE UNIVERSITY

MTI MINETA TRANSPORTATION INSTITUTE

# Is the Transit Industry Prepared for the Cyber Revolution? Policy Recommendations to Enhance Surface Transit Cyber Preparedness

Project 1939
September 2020

Scott Belcher, JD, MPP, Terri Belcher, Eric Greenwald, JD, and Brandon Thomas, MBA



Do you have a documented cybersecurity policy? If so, how often is it revised?

The U.S. Department of Homeland Security has designated the Transportation System Sector as one of 16 critical infrastructure sectors, whose disruption would have a debilitating effect on our nation's security. And yet, ransomware, data breaches, business email compromise and other cyber threats are on the rise, including among public transit agencies. In parallel, data flowing among vehicles, systems and vendors employed throughout the public transit industry too is growing. In short, the cybersecurity threat to public transit agencies is growing.

The intent of this study is to assess the readiness of public transit agencies to understand, mitigate, and respond to cybersecurity threats. This study reviews the state of best practices in cybersecurity among public transit agencies; outlines U.S. public transit operators' cybersecurity operations; assesses U.S. policy on cybersecurity in public transportation; and provides policy and operational recommendations.

## Study Methods

This study was based on a literature review; participation at industry meetings and conferences; expert interviews with transit operators, transit professionals, cybersecurity professionals and government officials; and a digital survey of public transit agency technology leaders.

## Findings

Just over 80% of agencies that responded to the digital survey believe they are prepared to manage and defend against cybersecurity threats, and yet only 60% have a cybersecurity program in place. There is an abundance of information and tools available to public transit agencies to support a cybersecurity program. Some transit agencies are aware of the risks posed and have taken actions to protect themselves. However, the digital survey data suggest this awareness is not industry-wide, and does not correlate to agency size, nor even if the agency had endured a substantive cybersecurity attack. Rather, agencies with effective cybersecurity programs have placed concerted focus and resources towards the threat, often hiring vendors and technical leadership from outside the public transit industry.

For the majority of transit agencies, cybersecurity will remain one of many important competing demands for limited resources. Until and unless the Federal government, the industry, and agency leadership work together to make cybersecurity a priority for transit agencies and provide the resources necessary to establish, maintain and refine cybersecurity programs, cybersecurity readiness will vary greatly among public transit agencies, ultimately putting the public at greater risk.

> *The survey findings demonstrate that many transit agencies do not fully appreciate the risks posed by cybersecurity vulnerabilities, nor the necessity to prepare for the inevitable attempts at a breach.*

## Policy Recommendations

**Executive Branch:** Develop cybersecurity standards and guidance for transit operators; require transit operators to attest to compliance with standards for funding.

**Legislature:** Provide funding for Executive Branch to develop standards and tools and ensure transit operators are resourced to implement the new requirements.

**Industry/Association:** Continue to develop, refine and improve existing guidance, best practices, and support materials and resources for transit operators to develop and make more robust their cybersecurity readiness.

## About the Authors

Scott Belcher, JD, MPP, is the CEO of SFB Consulting, LLC. Prior to founding SFB Consulting, LLC he served for two years as the CEO of the Telecommunications Industry Association and for seven years as the CEO of the Intelligent Transportation Society of America. Terri Belcher is a writer and policy analyst and has worked in Washington, D.C. for the past 30 years. Eric Greenwald, JD, most recently served as the General Counsel of Redacted, a cybersecurity firm. He joined Redacted from the White House, where he served as the Special Assistant to the President and Senior Director for Cybersecurity on the National Security Council (NSC). Brandon Thomas, MBA, is a Partner at Grayline Group, a firm focused on helping organizations understand and manage for disruption, as well as a Managing Partner of Blockview Partners, a firm focused on understanding the emerging blockchain and cryptocurrency space.

## To Learn More

For more details about the study, download the full report at transweb.sjsu.edu/research/1939

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.