Cybersecurity of Our Transportation Ecosystem

Identifying the Need

Cybersecurity has become a critical issue in today's world. In the past, security of our cyberspace was an important issue for select sectors of the economy -- those dealing with financial systems, corporate systems and trade secrets, government classified information, personal identification related, and other types of data that are considered valuable targets for hackers.

Transportation is not immune to the increase in cyber threats. Instead, it is likely to experience increased attacks. The reasons for this include:

- The aging nature of many of its systems
- The complex, heterogenous, and distributed nature of many field devices with limited security
- Significant advances in systems and technologies being researched and deployed (such as automated vehicles (AVs) and Cellular Vehicle-to-Everything (CV2X))
- Significant economic resources at risk (such as freight and pipeline operations)
- Significant safety implications (such as traffic management, maritime operations, or air traffic control)
- The potential for national scale disruptions that an attack could create.

Although transportation infrastructure is becoming progressively digitized and connected it continues to be a few steps behind other industries in its implementation of technology. Connectivity is often fragmented, and systems often remain in place with limited updates for decades. While cybersecurity efforts are generally improving, the opportunities and motivations for attack are increasing faster than our ability to defend against and build resiliency to attacks. Attacks themselves are changing, with increases in monetization and sophistication of attacks.

What is the goal?

The completed report examines trends in cyberattacks and cybersecurity, impacts on transportation, cybersecurity vulnerabilities, attack vectors including real-world instances of these attacks, and potential steps to address our transportation systems cybersecurity challenges.

Project Description

This project thoroughly investigates and reviews the California transportation system cybersecurity landscape, surveying state, regional, local, and private transportation system elements. It also gives suggestions on how we can secure our transportation system from cyberattacks. The report discusses ways in which our transportation system is vulnerable to cyberattacks, the level of risk of cyberattacks against our transportation system and risk trends, hypothetical and potential attack vectors, identification of potential threats, and possible impacts of cyberattacks against our transportation system. This project examines publicly available data on past attacks, both on the transportation sector and other sectors, as well as trends within the cybersecurity space.

Projected Benefits to California

The completed report discusses actions that transportation industry actors should take to limit both the likelihood and impact of a successful attack. It also discusses issues that impact an organizations' ability to improve their cybersecurity posture.

Due to the various nature of attacks and attackers, this report could serve as a guide to find any weak links and help protect and secure our transportation system infrastructure. This report intentionally does not include any information on existing cyber defenses specific to any individual organization or entity nor does it include any non-public information regarding past attack events to ensure we did not disclose any information that might increase the likelihood of any future attack.

What is the progress to date?

The project is complete. The project report is currently being reviewed by Caltrans. The completed report will be available on the PATH website after it has been finalized.

About the Author

Brian Peterson is a Systems Development Manager for the California Partners for Advanced Transportation Technology with over three decades of experience working in the engineering and software development industries. His distinguished career has included work in aircraft gas turbine maintenance and research, flight management systems, systems engineering, enterprise and large-scale real time systems, and software development programs. Brian has proven experience in both traditional and agile methodologies, systems engineering, and data management and standardization. His work continues to modernize and shape today's traffic management systems with California PATH-developed, leading-edge technologies.