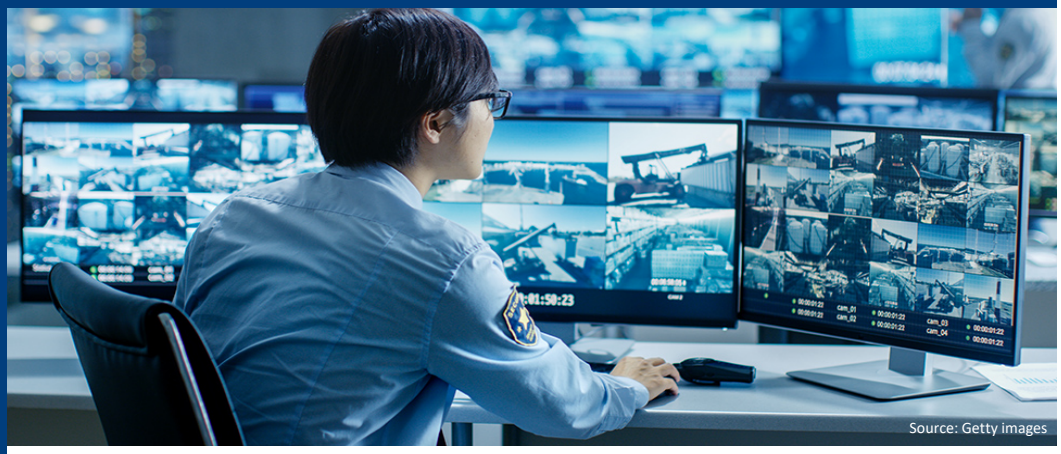
ITS DEPLOYMENT EVALUATION

Executive Briefing

Transportation Management Centers: Data and Cybersecurity



Highlights

- Coordinating and securing data through a TMC has the benefits of improving mobility, reducing environmental impacts, and increasing the overall safety of travelers.
- A TMC can make cyber-attacks harder by taking a "Defense in Depth" approach and interrupting as many of the attacker's steps as possible.

Table of Contents:

This brief is based on past evaluation data contained in the ITS Knowledge Resources database at: www.itskrs.its.dot.gov The database is maintained by the USDOT's ITS JPO Evaluation Program to support informed decision making regarding ITS investments by tracking the effectiveness of deployed ITS. The brief presents benefits, costs and lessons learned from past evaluations of ITS projects.

U.S. Department of Transportation
Intelligent Transportation Systems
Joint Program Office

Transportation Management Centers

Data and Cybersecurity

Introduction

Transportation or traffic management centers (TMCs) or transportation operations centers (TOCs) are an integral part of a transportation system. TMCs are responsible for operating the latest Intelligent Transportation System (ITS) technology including data collection, command and control of ITS devices, incident response, and communication for transportation networks. As deployments of ITS have increased over the last decade, state DOTs are continuing to implement TMCs to focus on the operations of their systems. TMCs are the focal point for agencies as they look to operate their transportation systems as efficiently as possible with the existing ITS infrastructure. New concepts are leading to the more effective use of conventional ITS devices in the field.

TMCs are going to be even more important in a connected vehicle, automated vehicle, and smart city environment. City TMCs are already operations centers that capture, analyze, and disseminate data. With the emergence of connected vehicles, TMCs will transform to be the hub for the collection of real-time data from both vehicles and infrastructure sending out traveler information and alerts to improve individual traveler's trips while also improving the full transportation system. TMCs can be the central data center of the transportation system of a city or region. Other recent initiatives and concepts such as Integrated Corridor Management (ICM) and Active Traffic and Demand Management (ATDM) have already started this trend with integrating more functionality into a single center for more responsive or even predictive traffic operation strategies. TMCs will be at the center of operating and maintaining these new systems.

Other technology trends that are impacting TMCs are big data, social media and crowdsourcing, and the continual growth of mobile and wireless communications. TMCs are collecting more and more data every day with the potential for data directly from vehicles in the near future. Social media is being used more and more for traveler information, while crowdsourced data is being used to gather data from drivers to obtain travel times, incidents, and other roadway information from driver reports [1].

ITS DEPLOYMENT EVALUATION

BENEFITS

Introduction (continued)

Smartphone applications, and soon, in-vehicle traveler information applications can provide real-time individualized traveler information to users through crowdsourced data and data collected and synthesized by TMCs. These applications are much more valuable with the TMC as the center hub, where operational decisions and traveler information can all come from the same agency. For example, data that in real-time can track the status of incidents on the roadway would be of great value to application developers and their end users [2].

As TMCs are collecting and analyzing the data to improve the overall transportation conditions, they are also becoming potential targets for cybersecurity attacks looking to disrupt or steal critical user information or Personal Identifiable Information (PII). To address this risk, transportation professionals that setup and maintain a TMC and its data must make security a top priority for the systems, devices, components, and protect communications from malicious attacks, unauthorized access, damage and disruptions that might interfere with system performance or functions.

Benefits

Coordinating and securing data through a TMC has the benefits of improving mobility, reducing environmental impacts, and increasing the overall safety of travelers. When multiple data sources are combined together additional benefits can be found versus single data sources. Examples could be weather and travel time, or speed and volume data.

Showing both safety and mobility benefits, the Wyoming DOT (WYDOT) TMC developed a Weather Responsive Traffic Management (WRTM) application by collecting and analyzing weather data to improve the way WYDOT maintenance personnel report road weather data, recommend variable speed limit changes and report traffic incidents.

This new application not only improved traffic conditions and increased safety, it also saved WYDOT an estimated one person-year in labor costs by stream-lining the data process (2017-01131).

This new application not only improved traffic conditions and increased safety it also saved WYDOT an estimated one person-year in labor costs by stream-lining the data process

Using a TMC as the information hub, Florida's Turnpike Enterprise deployed safety benefits through a ramp-based wrong-way driving detection and deterrent system (2017-01148). The system consisted of a front radar that is used to activate light-emitting diode (LED)-highlighted flashing signage when a vehicle enters the ramp in the wrong direction and triggers a camera to begin taking images. The TMC and Florida Highway Patrol (FHP) regional communications center continually monitor for an audible alarm with data checking approximately every 60 seconds, which is triggered when the web site is populated with event data. Since its inception, the system has successfully self-corrected all instances of wrong-way drivers, with zero crashes being reported during the pilot period.

Cameras tracking vehicles movement on highway

ITS DEPLOYMENT EVALUATION

BEST PRACTICES

Best Practices

The Road Commission for Oakland County (RCOC), Michigan, has maintained a real-time Traffic Management Center for more than 25 years, being one of the first local road agencies to introduce ITS technologies in the early 1990s. Its FAST-TRAC system is one of the largest traffic signal systems in North America. RCOC recently released a white paper summarizing its short- and long-term experiences in developing ITS expertise. A few of the best practices they highlighted were (2018-00849):

- When testing innovative technologies, start small and focus on the successes to consolidate a focused approach.
- Be prepared to test more technologies than you implement--only a few trials will materialize into field deployments.
- Customers expect real-time information and quick resolutions to any problems. It is important that they have relevant information at their fingertips.
- Personnel are important. Agencies should make an effort to properly train and retain qualified staff.
- Communications upgrades can be important for supporting future growth. They can also provide reduced down time, lower operational costs, augment system security, and support partnerships.
- It is possible to leverage public-private partnerships to maximize available agency funds for deployment and reinvestment.

WYDOT's experience in developing and integrating data from connected vehicles (CVs) into its TMC while considering the security, data management, and operator requirements highlighted the following practices and lessons learned (2019-00854).

- **Leverage existing open-source software** to integrate CV data into the TMC. WYDOT identified current efforts to develop software and worked in conjunction with developers to integrate open source software into the CV pilot project. This helped save significant time and yielded a more robust system, one built on top of previous experience.
- **Focus on the interfaces.** WYDOT's design approach highlighted the advantages of focusing on the specific interfaces the team needed to develop to send, receive and manage electronic messages or specific CV data. This strategy helped identify the gaps in existing systems, and the devices and changes needed to the TMC software and hardware platforms to enable the exchange and use of new data.
- **Have a "friendly" vehicle fleet (if possible).** WYDOT employed security and safety procedures to eliminate the tracking of all equipment or devices used for the pilot project (for example, equipment installed on participating commercial vehicles that are privately owned).
- **Translate CV data into information for the TMC**. WYDOT estimates the CV pilot project produces about 50 million electronic messages per day in addition to the 1 million already being generated by variable speed limit sensors and road weather information systems. To provide actionable data to TMC staff, the WYDOT TMC uses applications to translate raw CV data, such as basic safety messages, into discrete, useful information for TMC operators.
- **Create user-friendly dashboards and tools to monitor performance**. A clear need exists for dashboards to enable continuous monitoring of the various hardware and software that compose the CV pilot project.
- **Create a security and data management framework.** From the beginning, WYDOT envisioned a project that would follow "secure by design" principles that cover the process of forming, distributing, collecting, using, storing, and discarding data from CVs and TMC systems.
- **Involve broader State enterprise.** Integrating CV data into existing systems and operations requires a team effort with different skills to plan, design, develop, modify, and test the changes needed in both hardware and software systems.

ITS DEPLOYMENT EVALUATION

BEST PRACTICES

Best Practices (continued)

WYDOT not only leveraged efforts by other agencies and institutions, but also looked internally at its own systems and capabilities. WYDOT already had a robust network of data users and data suppliers—with its many traveler information outlets being visited and used by thousands of I-80 users on a daily basis—an efficient data distribution system, and a secure data archiving system.

- **Develop a critical path for development.** Wyoming's project deployed five applications on devices installed in vehicles along with updates to several components to WYDOT's traffic management and traveler information systems. Given the varying degree of interdependencies, WYDOT used an Agile development approach instead of the traditional waterfall approach (that is, in sequence) to develop this project. This enabled WYDOT to reach its goals within the tight schedule for development.

Forward thinking is needed to get ahead of security issues.

Cyber Security Challenges: Protecting your TMC

In response to Executive Order 13636, Improving Critical Infrastructure Cybersecurity, the U.S. Department of Transportation (USDOT) developed a Cyber Security Action Team to implement the Department's Incident Response Capability Program. The team leveraged U.S. transportation system security threat and vulnerability assessments and research conducted by the Federal Highway Administration (FHWA) staff and offered insights in a series of articles on transportation security that began in the July 2013 *ITE Journal* as outline below (2019-008567).

All networks can be breached and exploited, given enough time and resources. A TMC can make cyber-attacks harder by taking a "Defense in Depth" approach and interrupting as many of the attacker's steps as possible. The mitigation methods described below are based on Information Technology (IT) and e-commerce industry lessons learned, where losses frequently result in immediate and extensive economic losses with legal repercussions.

Stopping Breaches:

- **Assess risk.** Conduct full review of the data and system. Resources for determining risk include the Industrial Control Systems Cyber Emergency Response Team's Cyber Security Evaluation Tool (CSET).
- **Include TMC staff and staff** from other departments in social engineering risk evaluation, and train TMC management and staff to identify and defend against social engineering.
- **Implement network segmentation**, proper firewall deployment, and best practices in edge device communication.
- **Develop Information Security policy**, which TMC operators should understand and follow.
- **Have a visitor policy commensurate** with the perceived risk of the transportation system.

Disrupting Scans and Network Mapping:

- **Implement an Intrusion Detection System (IDS**) on the TMC internal network to detect abnormal behaviors from field devices and other network components.
- **Consider using a honeypot** to help trap intruders on the TMC's internal network and collect attack information for potential future prosecution against the attackers.
- **Encrypt communication** on the control network to make it more difficult for the attacker to understand the control system.

ITS DEPLOYMENT EVALUATION

BEST PRACTICES CASE STUDY

Best Practices (continued)

Limiting the Effects of Exploitation and Locking the Gate:

- **Execute a response plan** that is understood.
- **Monitor TMC data traffic between trusted partners** to prevent operational partners from becoming a source of unprotected backdoor attacks.
- **Limit data connections and connection types** into the internal TMC network to those required to maintain TMC operations.
- **Conduct and protect frequent backups** of critical applications and databases.
- **Keep parameters on the local controller current** for systems such as traffic signal control to allow local control to take over if the TMC is compromised.

Defending Against Denial Of Service (DOS) Attacks:

- **Stop an attack at the Internet Service Provider (ISP)** connection. DOS attacks typically come from the Internet.
- **Protect the Advanced Traveler Information Systems (ATIS)/511 server** as it is the target of most DOS attacks. Consider keeping the server separated from the internal network with a backend firewall.

Have a Plan:

- **Protecting a TMC's IT infrastructure deserves the same planning as addressing operational issues.** Planning will take time and help from the IT support group.
- **Planning resources** include The Roadmap to Secure Control Systems in the Transportation Sector [3], which was created to help agencies develop and sustain a plan, and resources from the IT industry.
- **Ensure the TMC and IT teams know how to execute the plan.**

Case Study

Colorado Department of Transportation Cyber Incident

Background

Between February 21-23, 2018, a threat actor executed a ransomware attack on the Colorado Department of Transportation (CDOT) that ultimately affected roughly half of the Department's computers. Despite immediate action by CDOT and Governor's Office of Internet Technology (OIT), CDOT suffered a second attack on March 1, 2018 that was discovered to pose risk to other state resources. On March 3, CDOT, OIT, and the Colorado Division of Homeland Security and Emergency Management (DHSEM) formed a Unified Command Group (UCG) to provide direction and control for incident responders. On March 8, the UCG completed Phase 1 (Containment) objectives and shifted to Phase 2 (Eradication) operations. On March 9, the UCG completed Phase 2 objectives and shifted to Phase 3 (Recovery) operations (2019-00856).

Root cause analysis revealed several vulnerabilities related to a newly created, Internet-accessible virtual server with direct connection into the CDOT network and administrative privileges that did not have OIT security controls in place.

This server was compromised within two days of creation and was under SamSam ransomware attack within one additional day.

Containment, eradication, and recovery of services required approximately four weeks.

Though CDOT operations were degraded, CDOT continued to execute its core mission to provide a multi modal transportation system for Colorado. This success may be attributed to a sound Continuity of Operations Plan that allowed CDOT to continue to operate and an OIT response that brought in the right people at the right time to contain and eradicate the threat. The creation of the UCG provided a clear direction and control structure that unified and focused the efforts of the numerous government agencies and private contractors involved. Though the State effectively responded to and recovered from this incident without paying the ransom, the threat to the State and its networks remains.

ITS DEPLOYMENT EVALUATION

CASE STUDY

Case Study (continued)

After Action Report

CDOT's experience offers various lessons regarding the hardening of networks, creating and rehearsing a cyber incident response plan, and allocating resources to both the necessary personnel and technology to effectively mitigate, respond to, and recover from future cyber-attacks.

Segment your network to isolate any potential malware. Network segmentation allowed OIT to isolate the malware within one department, protecting both the CDOT Intelligent Transit System and the cloud-based backup system.

Make the implementation of endpoint detection and response toolsets a top priority. While a Security Analytics and Endpoint Detection and Response toolset had recently been purchased, implementation was still being coordinated. If the toolset had been fully implemented, it would have alerted earlier and may have completely contained the outbreak.

Ensure there are no outdated systems in use that provide easy backdoors to attackers. A couple of outdated systems were discovered in the agency environment. The attackers utilized these outdated systems to establish staging environments and persistent backdoors into the environment.

Initiate protocols for centralized logging. OIT has a large logging initiative underway to ensure that all critical and essential systems and infrastructure components are sending security logs to a centralized log collection and analysis tool to filter the most significant security data.

Implement current system backups and segment them from the network. The successful FY17 completion of Colorado's system backup strategy, Backup Colorado, meant that OIT was confident in the offline backups of the servers and ability to recover data files. Backup Colorado was a key to successfully recovering from this incident and a significant factor in the decision not to pay the ransom.

Data security is critical for all parts of the network

Protect network diagrams and ensure familiarity with the agency network. Diagrams of the network were stored on systems which had been encrypted by the ransomware. As a result, incident response teams had to recreate the diagrams from memory and knowledge of the network.

Ensure that cyber incident response plans are fully integrated and operationalized. OIT has a cyber incident response plan and did use it for this incident, however the plan was not as operational as it could have been and was not rehearsed often enough to facilitate confident employment of the plan. As a result, a systematic approach to an escalating cyber incident did not exist.

References

1. *Impacts of Technology Advancements on Transportation Management Center Operations*. Federal Highway Administration, January 2013. http://www.ops.fhwa.dot.gov/publications/fhwahop13008/fhwahop13008.pdf.
2. *Transportation Management Center Data Capture for Performance and Mobility Measures Reference Manual*. Intelligent Transportation Systems Joint Program Office, March 27, 2013. https://rosap.ntl.bts.gov/view/dot/3373.
3. *The Roadmap to Secure Control Systems in the Transportation Sector.* The Roadmap to Secure Control Systems in the Transportation Sector Working Group, August 2012. https://ics-cert.us-cert.gov/sites/default/files/documents/TransportationRoadmap20120831.pdf